(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 289 326 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.03.2003 Bulletin 2003/10

(51) Int Cl.[7]: **H04Q 7/32**

(21) Application number: **01402259.4**

(22) Date of filing: **30.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Deloume, Pascal**
  31170 Tournefeuille (FR)
- **Garani, Pradeep**
  31000 Toulouse (FR)

(74) Representative: **Litchfield, Laura Marie et al**
Motorola European Intellectual Property Operations,
Midpoint - Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(54) Method of verifying downloaded software and corresponding device

(57) The present invention relates to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software. Thus the security of the keys and calculations involving the secure keys are kept secure. Preferably root security keys stored in the smart card can be updated using communication system messaging protocols.

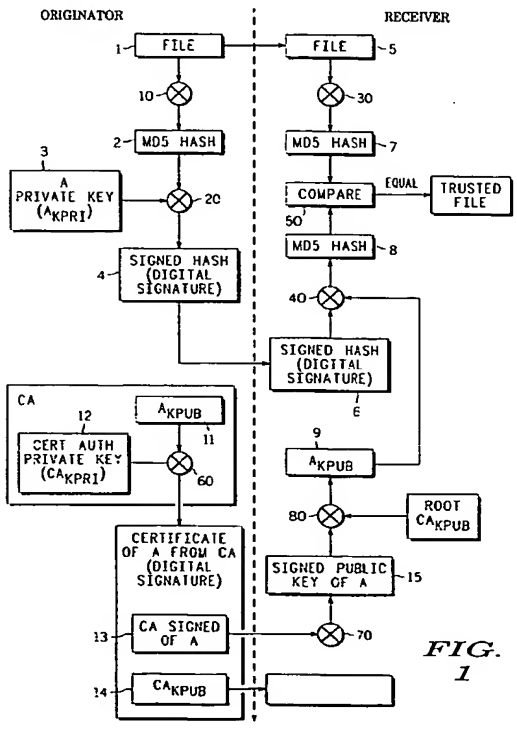


FIG. 1

EP 1 289 326 A1

Description

[0001] The present invention relates to a method of verifying software downloaded from an originator to a device, and to a corresponding device. In particular, the invention relates to download verification in standardised execution environments such as the Mobile Execution Environment (MExE) and Java.

[0002] Increasingly it is becoming desirable for software to be downloaded to a portable device over the air. This allows the device to be upgraded with newly released software or enables new applications to be added to the device as these become available.

[0003] It is desirable that the device checks the authenticity of the downloaded software to determine whether, for example, the downloaded software has indeed been received from a trusted sender. In addition, it is desirable that the downloaded software should be restricted to a given domain, to avoid permission violation for the rest of the device.

[0004] This security can be ensured by keys, which are stored securely in the device such that they cannot be read or tampered with by applications except the security-checking environment. In addition it is desirable to update the keys periodically, and this must be done using a secure method.

[0005] Previously, it has been suggested to implement the security algorithms in software/hardware and then to protect them by hardware control on the processor of the terminal with memory management unit. However, this results in increased cost. In addition, the development of separate security hardware is undesirable.

[0006] The Mobile Execution Environment (MExE), which enables software download, is currently under standardisation. Three class marks are defined in the MexE environment. Class mark 1 relates to devices utilizing the Wireless Application Protocol (WAP); class mark 2 relates to devices, such as personal digital assistants (pda) or laptops using standard edition JAVA™ (J2SE); and class mark 3 relates to small devices, such as mobile telephones, using micro-edition JAVA™ (J2ME).

[0007] J2ME is being proposed as an environment for class mark 3 devices in MExE because of its small size, which makes it suitable for environments, such as the mobile communication environment for example, in which the available memory or processing power is limited and the size of files must be limited.

[0008] However, the security model for J2ME requires server-based pre-verification, in which a server inserts basic run-time security information in the software prior to download. The receiving device can then use the run-time security information to check the security of the download and verify the sender.

[0009] It is desirable to increase the security provided for software download, particularly in a MExE class mark 3 environment, so that server-based verification is avoided and software can be downloaded from a greater variety of sources.

[0010] According to a first aspect of the present invention, there is provided a method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising: receiving software and security information relating to the received software; obtaining in the smart card a first calculation result from the security information using at least one secure key; obtaining in the device a second calculation result from calculations performed on the received software; and comparing in the device first and second calculation results to verify the received software.

[0011] According to a second aspect of the invention, there is provided a device comprising: communication means for receiving software and security information relating to the received software; smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key; means for obtaining a second calculation result from calculations performed on the received software; means for comparing first and second calculation results to verify the received software.

[0012] For a better understanding of the present invention, and to show how it may be brought into effect reference will now be made, by way of example to the accompanying drawings in which:

Figure 1 illustrates a known file transfer verification procedure;
Figure 2 shows a communication device;
Figure 3 illustrates a download verification procedure in accordance with the invention;
Figure 4 illustrates message creation for transfer of the root key in accordance with the invention;
Figure 5 illustrates update of the root key in accordance with the invention

[0013] The present invention is described with reference to the use of RSA cryptography. The RSA cryptography algorithm and principle are well known and therefore will not be explained in detail in this document. As will be apparent to a skilled person, other cryptography techniques may also be used in accordance with the invention.

[0014] Figure 1 illustrates a known file transfer verification procedure, for verifying the authenticity of a file transferred from an originator to a receiver. The principle behind this procedure is that in addition to the transfer of the file 1 a second piece of information which is related to both the file 1 and the originator is also transferred between the originator and the receiver, which information enables the receiver to confirm that the file comes from the originator. In addition, the receiver possesses or is passed a third piece of information, which enables

the receiver to confirm that the originator can be trusted and that it is therefore safe to execute the downloaded file.

[0015] In the illustrated procedure the originator generates the second piece of information by performing an MD5 hash operation 10 on the file 1 to be transferred to create an MD5 hash result 2. The MD5 hash operation is well known and will not be explained further. The MD5 hash result 2 is uniquely dependent on the file 1 and can be used to verify file 1.

[0016] Next the originator performs an RSA algorithm operation 20 on the MD5 hash result 2 using the private key of the originator (A_{KPRI}) 3 to generate a signed hash (or digital signature) 4. The signed hash 4 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 1 and the signed hash 4 are transferred to the receiver resulting in a received file 5 and a received signed hash 6.

[0017] In order to verify the received file, the receiver independently generates two versions of the MD5 hash result. The first MD5 hash result 7 is generated from the received file 5 using a MD5 hash operation 30, and the second MD5 hash result 8 is obtained from the received signed hash 6 by performing an RSA operation 40 on the received signed hash 6 using the public key of the originator A (A_{Kpub}) 9 held by the receiver. The first MD5 hash result 7 and the second MD5 hash result 8 are compared in a comparison operation 50 and if they are found to be equal, the received file 5 is authenticated and can be executed.

[0018] In order for the above authentication scheme to work, the receiver must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure through the use of a certification authority. The certification authority is trusted by the receiver, such that received information signed by the certification authority is trusted by the receiver.

[0019] Therefore, as shown the certification authority performs an RSA algorithm operation 60 on the public key of the originator (A_{KPub}) 11 using the private key of the certification authority (CA_{KPRI}) 12 resulting in a signed key 13 of the originator A. The signed key 13 and the certification authority public key (CA_{Kpub}) 14 are transferred to the receiver. As shown, if necessary the signed key 13 undergoes a certificate chain analysis operation 70 to obtain the received signed public key 15 of the originator A.

[0020] A certificate chain analysis operation is required if the certificate authority CA is not known by the receiver. In this case, the certificate authority is requested to provide its public key signed by a further certificate authority using the private key of the further certificate authority. If the further certificate authority is trusted by the receiver, the receiver will be able to use the public key of the further signature authority to verify that the public key of the signed authority has been signed by the private key of the further signature authority. The receiver can then trust the certificate authority and can use the received certificate authority public key. If the further certificate authority is not trusted by the receiver, use must be made of an additional certificate authority.

[0021] The receiver has stored therein a root certification authority public key. The root certification authority is the most trusted by the receiver, and ultimately the stored public key of the root certification authority can be used to verify all other certification authorities in a certificate chain situation.

[0022] The receiver then performs an RSA operation 80 on the resulting signed public key of the originator (A_{KPub}) (15) using the root certification authority public key (Root CA_{KPub}) to obtain the public key of the originator (A_{KPub}) 9. The public key of the originator (A_{KPub}) 9 is then used in the RSA operation 40 as described above.

[0023] The present invention is described below with reference to a communication device, such as a mobile telephone. However, it will be clear to a skilled person that the present invention is also applicable to other devices. An exemplary communication device 200 is now described with reference to Figure 2.

[0024] The communication device 200 shown in Figure 2 comprises a communication interface 210 coupled to an antenna 220 and to a processor 230. The processor 230 and the communication interface 210 are also coupled to volatile memory 240 and to a non-volatile memory 250. A smart card 260 is coupled to a smart card interface 270, which is also coupled to the processor 230. The smart card is equipped with its own processor 280 and memory 290.

[0025] The communication interface 210 comprises the necessary components to convert radio frequency signals for the communication device 200 received by the antenna 220 to digital signals to be stored in volatile memory 240 and/or non-volatile memory 250 and/or to be processed by processor 230, and to convert digital signals from the memories 240 and 250 and/or the processor 230 to radio frequency signals to be transmitted by the antenna 220. Thus communication interface 210 comprises radio frequency transmitter and receiver means and signal processor means, for example.

[0026] The volatile memory 240 and non-volatile memory 250 are used for storing program and other data for operation of the communication device 200.

[0027] The smart card is preferably a subscriber smart card (SIM) holding subscriber information used by the communication device 200, for example a Subscriber Identity Module card as currently used in the Global System for Mobile Communications (GSM system) and in use or proposed for other communication systems. However, it is possible that the smart card 260 may be another type of smart card received in the communication device instead of, or preferably in addition to a SIM card, for example an electronic commerce smart card.

[0028] As indicated above, the smart card is equipped with its own processor 280 and memory 290, and is capable of storing information therein and is also capable of carrying out operations or calculations on data received from the processor 230 via smart card interface 270 and of providing data or the results of such calculation to the processor 230 via smart card interface 270.

[0029] The smart card is preferably removably receivable in the communication device, for example by means of the provision of a slot in the housing of the communication device 200.

[0030] It will be appreciated by a skilled person that other components or arrangements of components within the communication device 200 are possible within the scope of the invention.

[0031] The secure download procedure in accordance with the invention will now be described with reference to Figure 3. In Figure 3 operations or data corresponding to operations or data in Figure 1 have been given similar reference numerals.

[0032] Figure 3 illustrates the download of an executable J2ME file in a MExE environment from an originator A to a device such as the communication device 200 described above with reference to Figure 2. As shown in Figure 3, box 3260 represents operations carried out and data stored in the smart card 260 of the communication device 200 shown in Figure 2, and the remaining operation and data storage is carried out in the rest of the communication device 200 shown in Figure 2.

[0033] As illustrated in Figure 2, the smart card 260 has no direct communications capability. Instead, the relevant data received by the communication device is passed by the processor 230 to the smart card 260 for storage therein and operation thereon.

[0034] In the procedure illustrated in Figure 3, the originator A performs an MD5 hash operation 310 on a file 31 to be transferred to create an MD5 hash result 32. As explained above, the MD5 hash result 32 is uniquely dependent on the file 31 and can be used to verify file 31.

[0035] Next the originator A performs an RSA algorithm operation 320 on the MD5 hash result 32 using the private key of the originator (A_{KPRI}) 33 to generate a signed hash 34. The signed hash 34 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 31 and the signed hash 34 are then sent to the communication device 200 resulting in a received file 35 and a received signed hash 36. File 35 is received using antenna 220 and communication interface 210 and is stored by the processor 230 in the volatile memory 240. In contrast, the signed hash 34 is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290.

[0036] As described above, in order to verify the received file, two versions of the MD5 hash result must be independently generated and compared. The first MD5 hash result 37 is generated by the communication device processor 230 from the received file 35 using a MD5 hash operation 330.

[0037] The second MD5 hash result 38 is obtained by the smart card from the received signed hash 36. The smart card processor 280 performs an RSA operation 340 on the received signed hash 36 stored in the smart card memory 390 using the public key of the originator A (A_{Kpub}) 39 stored in the smart card memory 290, as will be explained later.

[0038] The second MD5 hash result 38 is passed by the smart card processor 280 to the communication device processor 230 and the communication device processor 230 compares the first MD5 hash result 37 and the second MD5 hash result 38, calculated in the smart card 260, in a comparison operation 350. If the first MD5 hash result 37 and the second MD5 hash result 38 are found to be equal, the received file 35 is authenticated and can be executed.

[0039] In this arrangement, the smart card 260 must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure according to Figure 3 through the use of the root certification authority public key stored in the smart card memory 290. The root certification authority is trusted by the communications device, such that received information signed by the certification authority is trusted.

[0040] In this context, there may be more than one root certification authority. For example in the context of a mobile telephone the manufacturer and/or the operator can act as a root authority. In addition, it is possible to specify one or more trusted third parties as root certification authorities. The public key for each of the root certification authorities (eg the operator public root key (OPRK); the manufacturer public root key (MPRK); and third party public root key (TPRK)) is stored in the smart card of the communication device 200, for example during provisioning of a mobile telephone SIM card.

[0041] In order that the smart card 260 has authenticated access to the public key of the originator A (A_{Kpub}), as shown the root certification authority performs an RSA algorithm operation 360 on the public key of the originator (A_{KPub}) 311 using the private key of the certification authority ($RootCA_{KPRI}$) 312 resulting in a certificate from A 321 signed by the root certification authority. This certificate 321 is sent to the communications device 200, is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290 as certificate 322.

[0042] The Root certification authority public key ($RootCA_{KPub}$) 332 is already stored in the smart card memory 290, as indicated above. The smart card processor can perform an RSA operation 380 on the received certificate 322 using the Root Certification Authority public key ($RootCA_{KPub}$) 332 to obtain the public

key of the originator A (A_{Kpub}) 39. The smart card processor can then use the obtained public key of the originator A (A_{Kpub}) 39 and the received signed hash 36 in RSA operation 340 to obtain the smart card MD5 hash value 38, as outlined above.

[0043] Also shown in Figure 3 is the transfer of the Root Certification Authority public key ($RootCA_{KPub}$) 331 to the communications device for storage in the smart card memory as Root Certification Authority public key ($RootCA_{KPub}$) 332. It is desirable to update the root certification authority keys periodically in a secure manner otherwise the security of the system will be compromised.

[0044] A preferred mechanism for the secure transfer of a Root public key (for example OPRK, MPRK, TPRK) using communication system messaging technology will now be explained with reference to Figures 4 and 5.

[0045] Figure 4 illustrates message creation for transfer of a root key, for example the operator public root key (OPRK), to the smart card 360 in accordance with the invention. In this exemplary arrangement, the update is achieved using a SMS message as provided in the GSM/UMTS systems, although other messaging techniques could be used.

[0046] An RSA operation is performed on the new OPRK 41 with the operator's private root key 42 corresponding to the old OPRK stored in the smart card 360. As mentioned earlier, the old OPRK may have been stored in the smart card 360 during provisioning, or during a previous update of the root key. The resulting signed new operator public root key 44 is included in an SMS message 45 to be sent to the communication device. The SMS message 45 has an SMS header portion 451 and SMS download command 452 in addition to the signed new operator public root key 44. The SMS message in encrypted by the communication system prior to being sent to the communication device.

[0047] Figure 5 illustrates update of the root key in the communication device in accordance with an embodiment of the invention. In this exemplary embodiment of the invention, the SMS message 45 sent by the network 500 to the communication device 200 is passed to the smart card 260. Once the encrypted SMS message 45 is received in the smart card 260, the smart card 260 undertakes an SMS message analysis and memory update procedure 51.

[0048] In the SMS message analysis and memory update procedure 51 the SMS message is initially decrypted and the SMS message is analysed. The download command 452 instructs the smart card 260 that a new OPRK is being sent to the smart card 260. The smart card 260 performs an RSA operation on the received signed new OPRK using the old OPRK already stored in the smart card 260 to verify the identity of the sender. The OPRK stored in the smart card can then be updated using the new value. Preferably a confirmation message 52 is sent from the smart card 260 to the network using the communication interface 210 of the communication device 200.

[0049] Although the update of the operator public root key (OPRK) has been described above, it would be possible to update any root key stored in the smart card in the same way.

[0050] In accordance with an alternative embodiment of the invention, the manufacturer root public key may be stored partially in the smart card memory and partially in the communications device memory. This arrangement is more secure since the communication device then contributes to ensuring the security of download in the manufacturer domain using the manufacturer root public key. This helps to prevent an insecure smart card from changing the manufacturer public root key via download authorization.

[0051] Thus the present invention proposes a solution to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software.

[0052] Since the secure keys are stored on the smart card and calculations involving the secure keys are performed by the smart card, the security of the secure keys can be ensured. In addition, the result of the calculation performed on the received file by the device is not passed to the smart card.

[0053] As will be apparent to a skilled person, the invention could be implemented in a different form from that shown herein, and so the invention is intended to encompass all arrangements and variations within the scope of the appended claims.

Claims

1. A method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising:

   receiving software and security information relating to the received software;
   obtaining in the smart card a first calculation result from the security information using at least one secure key;
   obtaining in the device a second calculation result from calculations performed on the received software; and
   comparing in the device first and second calculation results to verify the received software.

2. The method as claimed in claim 1, further comprising the steps of;

   receiving additional signed originator key infor-

mation;

obtaining, in the smart card, originator key information from the received signed originator key information using a root security key stored therein; and

obtaining in the smart card the first calculation result from the security information using the originator key information.

3. The method as claimed in claim 2 wherein the root security key stored in the smart card is updated by

receiving a root security key update message containing a new root security key;

verifying the new root security key using the existing root security key stored in the smart card;

storing the new root security key in the smart card.

4. The method as claimed in claim 2 or 3, wherein part of the root security key is stored in the smart card and part of the root security key is stored in the device.

5. The method as claimed in any preceding claim, wherein the smart card is a Subscriber Identity Module (SIM) card

6. A device comprising

communication means for receiving software and security information relating to the received software;

smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key;

means for obtaining a second calculation result from calculations performed on the received software;

means for comparing first and second calculation results to verify the received software.

7. The device as claimed in claim 6 wherein

the communications means also receives additional signed originator key information; and

the smart card interface also passes the additional signed originator key information to the smart card, which obtains originator key information from the received signed originator key information using a root security key stored therein; and obtains the first calculation result from the security information using the originator key information.

8. The device as claimed in claim 7 wherein

the communications means also receives a root security key update message containing a new root security key; and

the smart card interface passes the root security key update message to the smart card, which verifies the new root security key using the existing root security key stored in the smart card; and stores the new root security key in the smart card.

9. The device as claimed in claim 7 or 8, wherein the device comprises storage means and part of the root security key is stored in the smart card and part of the root security key is stored in the storage means.

10. The device as claimed in one of claims 6-9, wherein the smart card is a Subscriber Identity Module (SIM) card.

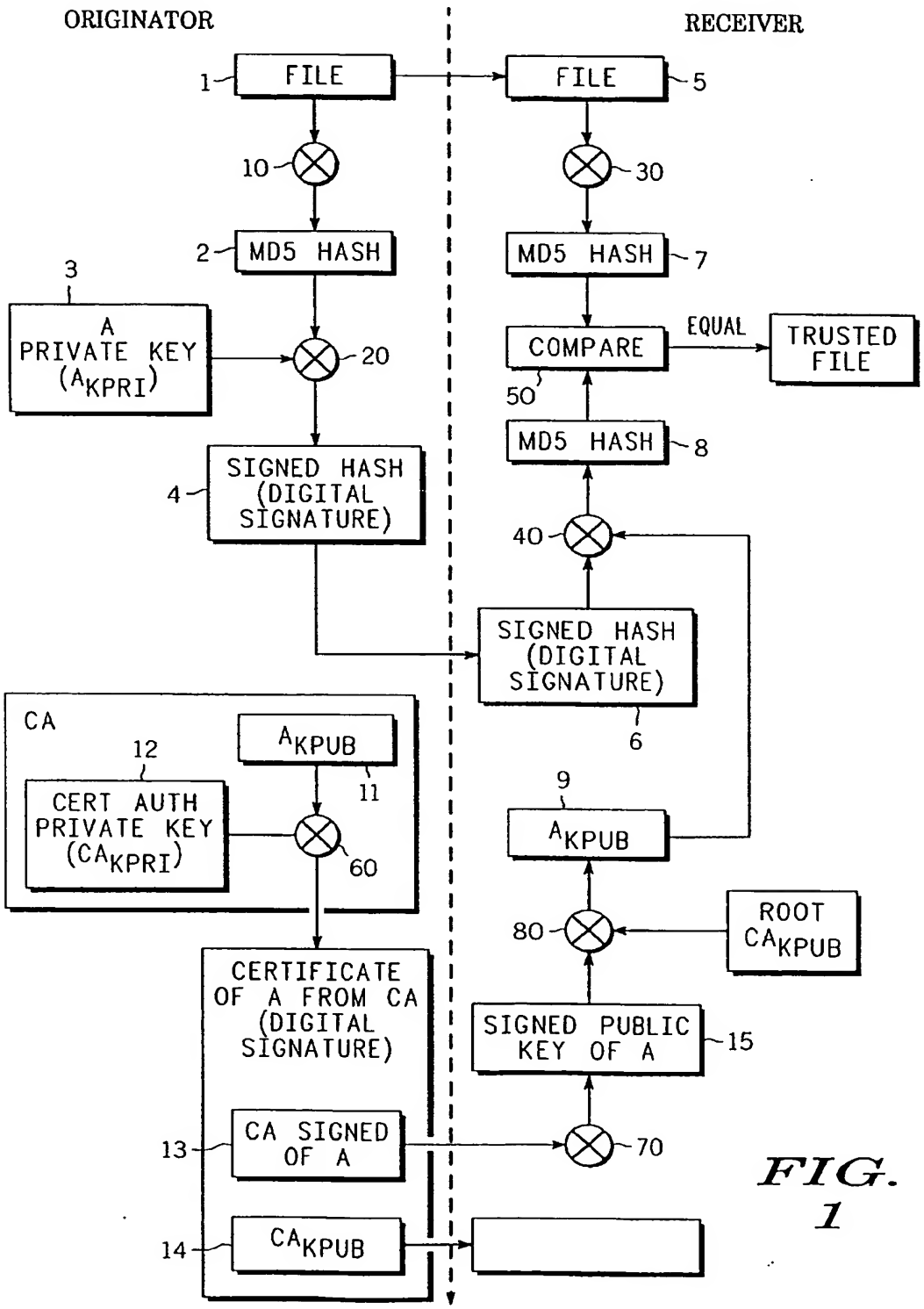

ORIGINATOR
RECEIVER
1
FILE
FILE
5
10
30
2
MD5 HASH
MD5 HASH
7
3
A PRIVATE KEY (A_{KPRI})
20
COMPARE
EQUAL
TRUSTED FILE
50
MD5 HASH
8
4
SIGNED HASH (DIGITAL SIGNATURE)
40
SIGNED HASH (DIGITAL SIGNATURE)
6
CA
A_{KPUB}
12
11
9
CERT AUTH PRIVATE KEY (CA_{KPRI})
60
A_{KPUB}
80
ROOT CA_{KPUB}
CERTIFICATE OF A FROM CA (DIGITAL SIGNATURE)
SIGNED PUBLIC KEY OF A
15
13
CA SIGNED OF A
70
14
CA_{KPUB}

FIG. 1

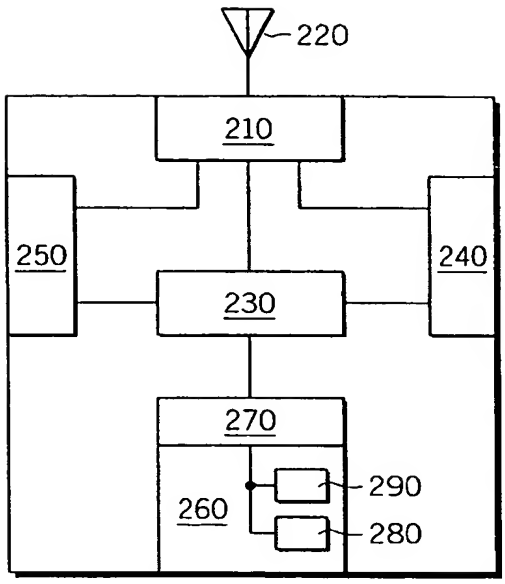


FIG. 2

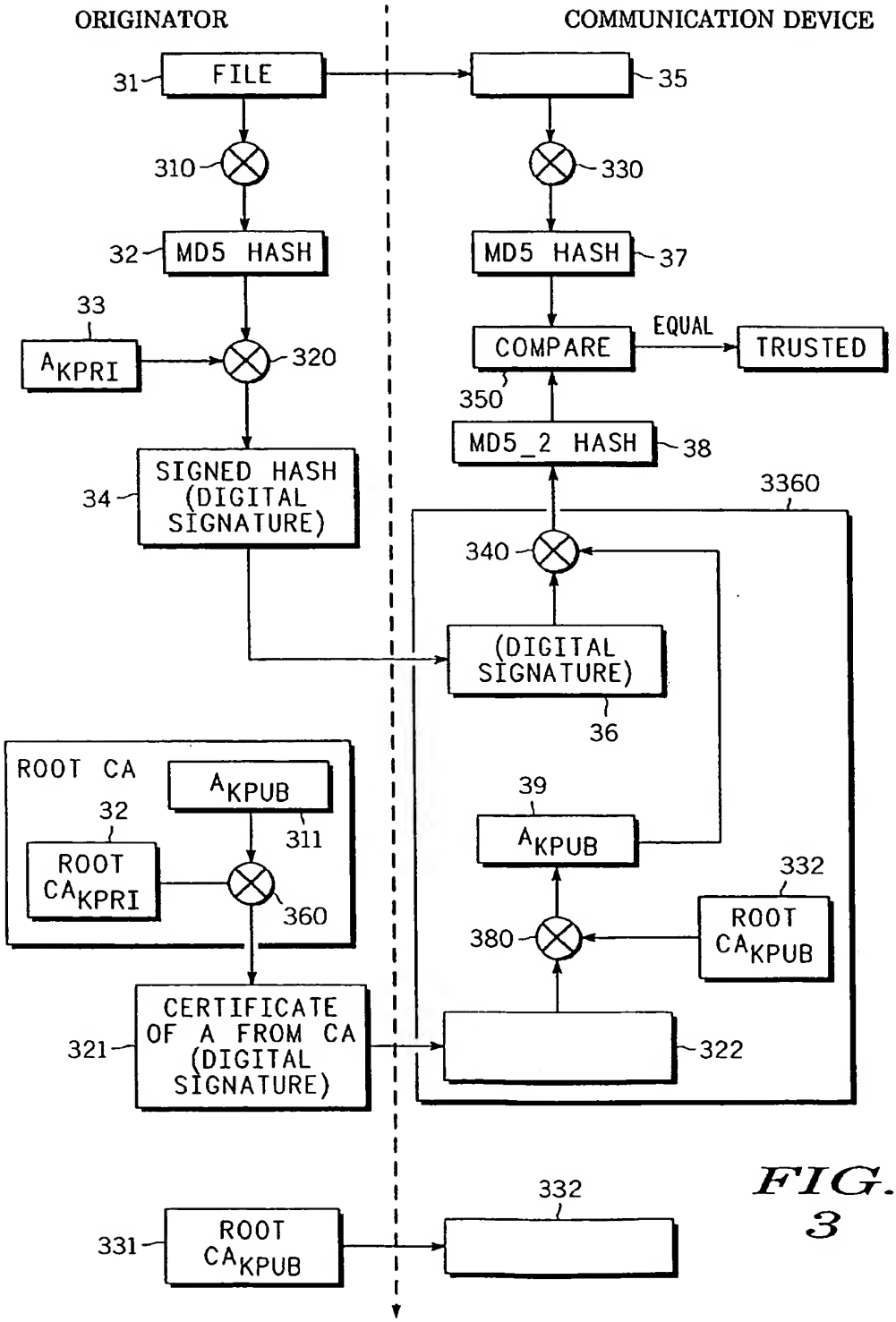

ORIGINATOR
COMMUNICATION DEVICE
31
FILE
35
310
330
32
MD5 HASH
MD5 HASH
37
33
A_{KPRI}
320
COMPARE
EQUAL
TRUSTED
350
MD5_2 HASH
38
34
SIGNED HASH (DIGITAL SIGNATURE)
3360
340
(DIGITAL SIGNATURE)
36
ROOT CA
A_{KPUB}
32
311
39
A_{KPUB}
ROOT CA_{KPRI}
360
332
380
ROOT CA_{KPUB}
CERTIFICATE OF A FROM CA (DIGITAL SIGNATURE)
321
322
331
ROOT CA_{KPUB}
332

FIG. 3

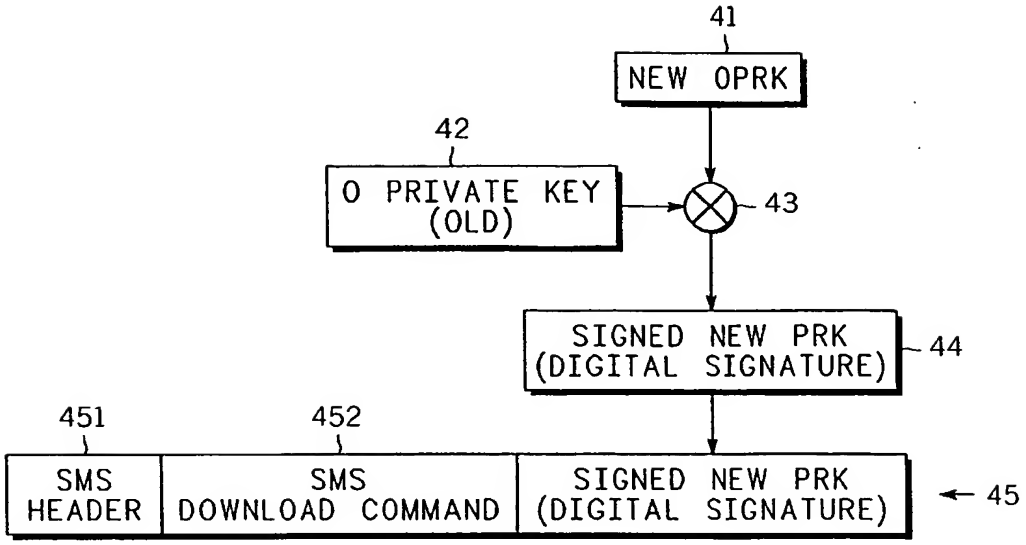
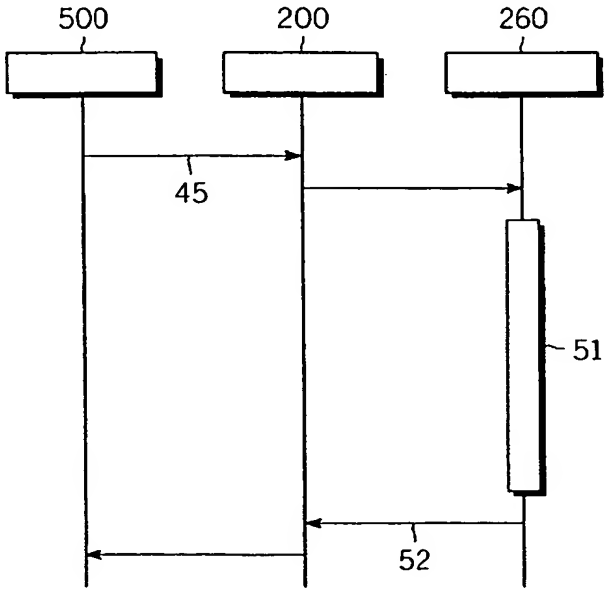

41
NEW OPRK
42
O PRIVATE KEY (OLD)
43
SIGNED NEW PRK (DIGITAL SIGNATURE)
44
451
452
SMS HEADER
SMS DOWNLOAD COMMAND
SIGNED NEW PRK (DIGITAL SIGNATURE)
45

FIG. 4

FIG. 5


500
200
260
45
51
52

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2259

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 124 799 A (PARKER JOHN PATRICK) 26 September 2000 (2000-09-26) * the whole document *	1-4,6-9	H04Q7/32
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) * column 4, line 30 - column 5, line 32 *	1,6	
A	EP 1 124 401 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) * paragraphs '0002!-'0019! * * abstract; claims 1-13 *	2-4,7-9	
A	EP 0 977 452 A (LUCENT TECHNOLOGIES INC) 2 February 2000 (2000-02-02) * the whole document *	2-4,7-9	
A	EP 0 463 384 A (CIT ALCATEL) 2 January 1992 (1992-01-02) * the whole document *	1,6	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 February 2002	Coppieters, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2259

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-02-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6124799 A	26-09-2000	US 5864757 A	26-01-1999
		AU 715488 B2	03-02-2000
		AU 1409997 A	03-07-1997
		CA 2239550 A1	19-06-1997
		EP 0867099 A2	30-09-1998
		JP 11501182 T	26-01-1999
		JP 3080409 B2	28-08-2000
		WO 9722221 A2	19-06-1997
EP 0562890 A	29-09-1993	AT 193965 T	15-06-2000
		DE 69328847 D1	20-07-2000
		DE 69328847 T2	07-12-2000
		EP 0562890 A1	29-09-1993
		ES 2149801 T3	16-11-2000
EP 1124401 A	16-08-2001	AU 1828001 A	16-08-2001
		BR 0100191 A	09-10-2001
		CN 1308472 A	15-08-2001
		EP 1124401 A2	16-08-2001
		JP 2001251292 A	14-09-2001
EP 0977452 A	02-02-2000	US 6243811 B1	05-06-2001
		BR 9902942 A	09-05-2000
		CN 1249588 A	05-04-2000
		EP 0977452 A2	02-02-2000
		JP 2000083017 A	21-03-2000
		TW 428409 B	01-04-2001
EP 0463384 A	02-01-1992	FR 2662878 A1	06-12-1991
		AT 135519 T	15-03-1996
		CA 2043290 A1	01-12-1991
		DE 69117814 D1	18-04-1996
		DE 69117814 T2	25-07-1996
		EP 0463384 A1	02-01-1992
		ES 2084726 T3	16-05-1996
		FI 912548 A	01-12-1991
		JP 3054225 B2	19-06-2000
		JP 4233341 A	21-08-1992
		NO 178597 B	15-01-1996
		US 5303285 A	12-04-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 326 396 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.07.2003 Bulletin 2003/28

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **02026429.7**

(22) Date of filing: **26.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.11.2001 JP 2001359940**
05.11.2002 JP 2002321844

(71) Applicant: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
Kadoma-shi, Osaka 571-8501 (JP)

(72) Inventor: **Minemura, Atsushi**
Tokyo 174-0074 (JP)

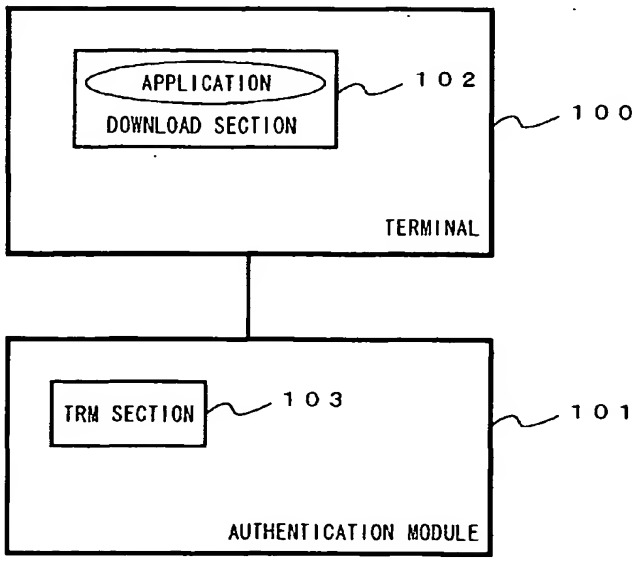
(74) Representative: **Betten & Resch**
Patentanwälte,
Theatinerstrasse 8
80333 München (DE)

(54) Application authentication system

(57) Since there is a possibility that an application downloaded to a terminal performs an invalid operation, an operation of the downloaded application is very much restricted, and the application cannot use local resources of the terminal

With the use of information for authenticating the application, which is held in a tamper-resistant region of an authentication module, authentication for the application downloaded to a download section of the terminal is performed to confirm its source or whether or not it has been tampered with. Only an authenticated application is permitted to use the local resources of the terminal or the authentication module, so that an invalid application is prevented from using the local resources. Further, there is no need to make the terminal have the tamper-resistant region, manufacturing costs of the terminal can be held at a low level.

FIG. 1



EP 1 326 396 A2

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to technology to authenticate a terminal and an application program that operates in the terminal, in a system having a terminal such as a cell phone and an authentication module such as an IC card.

Description of the Prior Art

[0002] Conventionally, in a system where the IC card is attached to the terminal to perform business transaction with a server, an application program (hereinafter, abbreviated as 'application') operating in the server has directly authenticated the IC card because a region having tamper-resistance cannot be secured in the terminal. Therefore, the terminal has only relayed communication between the server and the IC card.

[0003] On the other hand, it has been made possible in recent years for the server to download the application to a cell phone or the like to operate it in a portable terminal.

[0004] However, since there is a possibility that the application downloaded to the cell phone performs an invalid operation, an operation of the downloaded application is very much restricted.

[0005] For example, use of local resources is greatly restricted for the application downloaded to the cell phone, such that it cannot write data in the IC card attached to the cell phone and use of various kinds of interfaces is restricted (prohibited).

[0006] Further, the application downloaded to the cell phone is restricted to reading and writing of personal information such as a mail address recorded in a telephone book or an address book or contents of mails stored in a mail inbox, which is held by the cell phone or the IC card. This is because the relevant application is an authorized one, and verification, whether or not it has a right to access to the information held inside the cell phone, the IC card or the like, or whether or not it operates obliquely, cannot be performed.

[0007] This could be an extremely large disincentive to all-purpose use (versatility) of portable tools and applications to E-commerce (EC), which have promising futures.

[0008] To eliminate the restrictions, the downloaded application needs to be authenticated to confirm a feature of the application. For example, a signature that a third person has added to the application is downloaded along with the application, the signature and information necessary for verifying correctness of the signature are presented to the IC card, and thus authentication is performed. However, since the cell phone generates the information (a digest generated by a hash function, for example) necessary for determining the correctness of the signature after the cell phone has downloaded the application and the signature, there is a possibility that a dummy signature, which is different from the signature added to the downloaded application, and a digest, which has been manipulated such that verification can be performed by the signature, are presented to the IC card by the cell phone. For this reason, there exists a problem that the IC card cannot trust that the signature and the digest presented to the IC card are actually the ones of the downloaded application, and the IC card cannot perform authentication for the downloaded application.

[0009] Furthermore, to enable the application downloaded to the terminal such as a cell phone (hereinafter, abbreviated to a 'terminal application') to access to the IC card and to read and write the information stored in the IC card so as to be protected, it is required that a processing for authenticating the terminal application that accesses the IC card is similarly performed by the IC card to determine whether or not access may be permitted.

[0010] As processing where a secure device such as the IC card performs authentication for the terminal application that accesses the IC card, processing has conventionally been performed so that the secure device determines whether or not the terminal application has secret information similar to information held therein. However, the terminal does not have a region or a function such as a region having tamper-resistance for securely holding the secret information. For this reason, there exists a problem that the secret information may leak and the conventional method cannot eliminate the possibility that the terminal application uses the leaked information and thus the secure device cannot authenticate the terminal application closely.

SUMMARY OF THE INVENTION

[0011] To solve the aforementioned problems, the present invention allows the tamper-resistant region in the authentication module such as the IC card to have information for authenticating a program written in the ROM of the terminal such as a cell phone (hereinafter, the program may be referred to as a 'library'), and the authentication module performs authentication for a library written in a region such as the ROM and a TRM of the terminal, whose rewriting is difficult.

[0012] When the library authenticated in this manner spontaneously generates necessary information to determine the correctness of the signature and presents it to the IC card along with the signature of the downloaded application, the IC card can trust that the signature and the information presented by the authenticated library are actually the ones of the downloaded application, and thus the IC card can authenticate the application downloaded to the terminal. As the result, the authenticated application can write data in the IC card,

which can realize a more complicated operation than the operation of business transaction using a conventional terminal.

[0013] Further, by authenticating the application downloaded to the terminal with the IC card as described-above, it becomes possible that the downloaded application is allowed to use an external interface of the terminal.

[0014] To execute the present invention, the signature of the application to be downloaded needs to be downloaded. Therefore, it is made possible that the signature of the application is not only downloaded independently of the application, but also stored in a definition file of the application in order to deal with conventional data specification. Accordingly, downloading of the signature independently of downloading of the application is unnecessary.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings.

[0016] Fig. 1 is a function block diagram of an application authentication system in the first embodiment in the present invention.

[0017] Fig. 2 is a view showing an example of the application authentication system in the first embodiment of the present invention.

[0018] Fig. 3 is a view showing another example of the application authentication system in the first embodiment of the present invention.

[0019] Fig. 4 is a function block diagram of the application authentication system in the second embodiment of the present invention.

[0020] Fig. 5 is a function block diagram of an application authentication system in the second embodiment of the present invention.

[0021] Fig. 6 is a view explaining an application main body and a signature.

[0022] Fig. 7 is a flowchart explaining an operation of a terminal in the second embodiment of the present invention.

[0023] Fig. 8 is a flowchart explaining an operation of an authentication module in the second embodiment of the present invention.

[0024] Fig. 9 is a function block diagram of the authentication module in the third embodiment of the present invention.

[0025] Fig. 10 is a flowchart explaining the operation of the authentication module in the third embodiment of the present invention.

[0026] Fig. 11 is a function block diagram of the application authentication system in the fourth embodiment of the present invention.

[0027] Fig. 12 is a flowchart explaining a processing where a terminal authenticates the authentication module in the fourth embodiment of the present invention.

[0028] Fig. 13 is a function block diagram of the application authentication system in the fifth embodiment of the present invention.

[0029] Fig. 14 is a view schematically showing application-usable resource information.

[0030] Fig. 15 is a view schematically showing a state where the application-usable resource information is downloaded with an application.

[0031] Fig. 16 is a function block diagram of the application authentication system in the sixth embodiment of the present invention.

[0032] Fig. 17 is a function block diagram of the application authentication system in the seventh embodiment of the present invention.

[0033] Fig. 18 is a function block diagram of the application authentication system in the eighth embodiment of the present invention.

[0034] Fig. 19 is a flowchart explaining an operation of the terminal in the eighth embodiment of the present invention.

[0035] Fig. 20 is a flowchart explaining an operation of the authentication module in the eighth embodiment of the present invention.

[0036] Fig. 21 is a function block diagram of the application authentication system in the ninth embodiment of the present invention.

[0037] Fig. 22 is a flowchart explaining an operation of the authentication module in the ninth embodiment of the present invention.

[0038] Fig. 23 is another flowchart explaining an operation of the authentication module in the ninth embodiment of the present invention.

[0039] Fig. 24 is another function block diagram of the application authentication system in the ninth embodiment of the present invention.

[0040] Fig. 25 is a view showing an example where the ninth embodiment of the present invention is realized in an IC card.

[0041] Fig. 26 is a view showing another example where the ninth embodiment of the present invention is realized in an IC card.

[0042] Fig. 27 is a function block diagram of the application authentication system in the tenth embodiment of the present invention.

[0043] Fig. 28 is a function block diagram of the application authentication system in the eleventh embodiment of the present invention.

[0044] Fig. 29 is a function block diagram of the application authentication system in the twelfth embodiment of the present invention.

[0045] Fig. 30 is a sequential diagram explaining an operation of the application authentication system in the twelfth embodiment of the present invention.

[0046] Fig. 31 is a function block diagram of the application authentication system in the thirteenth embodiment of the present invention.

[0047] Fig. 32 is a sequential diagram explaining an

operation of the application authentication system in the thirteenth embodiment of the present invention.

[0048] Fig. 33 is a function block diagram of the application authentication system in the fourteenth embodiment of the present invention.

[0049] Fig. 34 is a view schematically showing an application main body and an application definition file of a Java application.

[0050] Fig. 35 is a flowchart explaining a processing of application authentication by using a signature stored in an optional region.

[0051] Fig. 36 is a view in which the TRM access library section of the application authentication system of the second embodiment has an application manger and a device driver.

[0052] Fig. 37 is a function block diagram of the terminal of the sixteenth embodiment of the present invention.

[0053] Fig. 38 is a function block diagram of the terminal of the seventeenth embodiment of the present invention.

[0054] Fig. 39 is a flowchart explaining a processing flow in the terminal of the seventeenth embodiment.

[0055] Fig. 40 is a function block diagram of the application authentication system in the eighteenth embodiment of the present invention.

[0056] Fig. 41 is a function block diagram of the application authentication system in the nineteenth embodiment of the present invention.

[0057] Fig. 42 is a flowchart explaining a processing flow of the application authentication system in the nineteenth embodiment of the present invention.

[0058] Fig. 43 is a function block diagram of the application authentication system that consists of three kinds of equipment.

[0059] Fig. 44 is a flowchart explaining an operation flow of the first equipment.

[0060] Fig. 45 is a flowchart explaining an operation flow of the second equipment.

[0061] Fig. 46 is a flowchart explaining an operation flow of the third equipment when the application authentication system consists of the three kinds of equipment.

[0062] Fig. 47 is a function block diagram of the application authentication system that consists of four kinds of equipment.

[0063] Fig. 48 is a flowchart explaining an operation flow of the third equipment when the application authentication system consists of the four kinds of equipment.

[0064] Fig. 49 is a flowchart explaining an operation flow of the fourth equipment when the application authentication system consists of the four kinds of equipment.

[0065] Fig. 50 is a function block diagram of the application authentication system that consists of five kinds of equipment.

[0066] Fig. 51 is a function block diagram of the application authentication system that consists of N+1 kinds of equipment.

[0067] Fig. 52 is a flowchart explaining an operation flow of the i-th equipment.

[0068] Fig. 53 is a flowchart explaining an operation flow of the (N+1)th equipment.

[0069] Fig. 54 is a schematic diagram showing that the equipment is connected using a nested structure.

[0070] Fig. 55 is a flowchart explaining an operation flow of the i-th equipment in the twenty-first embodiment of the present invention.

PREFERRED EMBODIMENTS OF THE INVENTION

[0071] The present invention relates to the application authentication system that includes the terminal and the authentication module, and the 'terminal' may be a portable electronic device represented by the cell phone. Further, it also may be a personal computer or a public terminal installed on a street corner, which is virtually not portable. It is an electronic device to which the authentication module described below is attachable, and it can operate the application inside the device. The terminal has various kinds of sections inside as described below, and these sections can be realized by software when the terminal is provided with a ROM, a RAM and a CPU.

[0072] The 'authentication module' is one having a storage area inside, which is a (SD) memory card, an IC card or a smart card, and it performs an operation to reply to data entered when the data is entered from the terminal to which the module is attached. Furthermore, the authentication module has a region called a tamper-resistant region that prevents invalid reading-out and invalid rewriting of information stored therein. A few of the sections in the authentication module described below can also be realized by a card application that operates in such an IC card.

[0073] Generally, the authentication module is attached to the terminal, and an electrical circuit is formed between the terminal and the authentication module to exchange information. However, there also exists a mode where the main body of the terminal and a part to which the authentication module is attached separately, and information is exchanged by communication.

[0074] Note that the application operating on the terminal performs one or more arithmetic operations, use a local interface, access the server, access the tamper-resistant region, and access an external memory. The 'local interface' is an external interface that the terminal has, where IrDA (an interface for infrared communication), Bluetooth, another radio communication, an interface for cable communication, and the like are cited.

[0075] Note that description has been made above that the terminal and the authentication module are easily separated, but the terminal may be provided inside the terminal so as to be crimped or soldered to the terminal circuit so that they cannot be separated easily.

[0076] Further, although description 'terminal' has been made above, the present invention is not limited

to portable equipment and can be executed by using a personal computer, a workstation, or the like, instead of the terminal.

[0077] Furthermore, the present invention can be applied to a processing that, in a state that a plurality of equipment are connected in series, equipment on one end performs authentication for the application stored in equipment on the other end.

First Embodiment

[0078] Fig. 1 is the function block diagram of the application authentication system in the first embodiment in the present invention. The application authentication system in this embodiment has a terminal 100 and an authentication module 101.

[0079] The terminal 100 has a download section 102 that downloads the application. 'To download the application' is to read in data for executing the application from outside of the download section 102. Herein, 'data for executing the application' is: binary data, if the application is the binary data directly executable by the terminal 100; and description of a language, if the application is described in the language interpreted and executed by the terminal 100. The download section reads in the data for executing the application and holds the data.

[0080] The authentication module 101 has a TRM section 103. The TRM section 103 holds information for a processing of application authentication in the tamper-resistant region. Note that the 'TRM' is the abbreviation for a 'Tamper Resistant Module'. The 'application' is an application downloaded to the download section 102 of the terminal 100, and the 'application authentication' is to confirm that the application does not perform an invalid operation such as whether or not the application has been issued by a credible person, has been guaranteed not to perform an invalid operation, or has been tampered after it was issued by the credible person or has been tampered with after it was guaranteed not to operate obliquely. The 'processing the application authentication' is a processing to confirm such authentication.

[0081] As a method of processing the authentication, a hash function (may be referred to as a 'digest function' instead of the 'hash function') such as a SHA-1 (Secure Hash Standard-1) and a MD5 (Message Digest 5) is generally used to find resultant data that is obtained after processing the data for executing the application as input data, and the encrypted data (a so-called 'signature') is used. Herein, the 'hash function' is a function that returns a result, where finding two different input data such that the resultant data obtained after processing the input data match is difficult from a complexity point of view. Therefore, the 'information for processing the application authentication' is the actual signature or a decryption key necessary for decrypting the signature to obtain a hash value. The 'tamper-resistant region' is a storage area of the authentication module, which is a storage area whose data is difficult to read out or rewrite in an invalid manner. Such a storage area is realized in such a manner that a user must go through hardware that is not accessible unless the user takes a right procedure to access to the storage area, or that the data stored in the storage area is encrypted.

[0082] In the application authentication, the terminal 100 finds the hash value of the application downloaded to the download section 102, presents the signature for the authentication module 101 along with the hash value, and the authentication module 101 checks with the information held in the TRM section 103 whether or not the signature can be generated from the hash value or the hash value matches a hash value obtained by decrypting the signature. Further, the terminal 100 presents the actual application downloaded to the download section 102 and the signature for the authentication module 101, and may check the relationship between the actual application and the signature to perform authentication.

[0083] With the application authentication system of this configuration, the application downloaded to the download section 102 can be authenticated by the information held in the TRM section 103 of the authentication module 101. Thus, the system can prevent downloading of an invalid application to be executed in the terminal 100 or stored in the authentication module 101.

[0084] Fig. 2 shows an example of the application authentication system in this embodiment. In this example, a service retailing company 200 distributes the authentication module 101 in a state that an application 201 is stored therein. When a person who has obtained the authentication module 101 attaches the module 101 to the terminal 100, the application 201 is downloaded from the authentication module 101 to the download section 102 of the terminal 100 (arrow 203). When an downloaded application 202 is authenticated by the information stored in the TRM section of the authentication module 101, the application 202 operates in the terminal 100 to receive provision of service from the service retailing company 200 (arrow 204).

[0085] Fig. 3 shows another example of the application authentication system in this embodiment. In this example, the service retailing company 200 downloads an application 302 to the download section 102 of the terminal (arrow 303). When authentication is performed to the application 302 by the information held in the TRM section of the authentication module 101 and confirmation is made that the application is not an invalid application, it is stored as an application 301 in the authentication module 101 (arrow 304). Then, the application 301 is downloaded to the download section 102 of the terminal 100 if necessary, and executed in the terminal 100.

[0086] In Figs. 2 and 3, although the application executed in the terminal 100 is downloaded from the authentication module 101, another example is cited as fol-

lows. When a server, to which the terminal 100 has connected, downloads the application, authentication is performed by the information held in the TRM section of the authentication module 101, and confirmation is made that the application is not an invalid application, the application is executed in the terminal 100.

[0087] Although the word 'terminal' has been used, it does not mean that the word is limited to the portable terminal or the like represented by the cell phone. For example, it may be a home electronic appliance, and also may be a so-called information home electronic appliance or a network home electronic appliance. Products such as an air conditioner, a humidifier, a dehumidifier, an air cleaner, a microwave oven, an oven, a refrigerator, a dish washing machine, a water heater, an iron, a trouser press, an electric vacuum cleaner, a washing machine, a drier, an electric blanket, electric sheets, a light fixture, a television, a radio, an audio apparatus such as a tape recorder, a camera, an IC recorder, a telephone, a facsimile machine, a copier, a printer, a scanner, a personal computer, and the like are cited.

Second Embodiment

[0088] Fig. 4 shows a function block diagram of the application authentication system in the second embodiment of the present invention, and the application authentication system comprises the terminal 100 and the authentication module 101. The terminal 100 has the download section 102 and a TRM access library section 401. The authentication module 101 has the TRM section 103 and a TRM access library section authenticating section 402.

[0089] The download section 102 downloads the application.

[0090] The TRM access library section 401 performs a processing for application authentication on condition that it is authenticated by the authentication module 101. Specifically, the TRM access library section 401 makes the authentication module 101 perform authentication for the section 401 itself first, and performs processing for application authentication when it is authenticated correctly.

[0091] As a method that the TRM access library section 401 makes the authentication module 101 perform authentication for the section 401 itself, there exists a method where information unique to the terminal 100 is output to the authentication module 101, and the authentication module 101 checks whether or not the output information matches the information stored in the tamper-resistant region to perform authentication. As the 'information unique to the terminal 100', (1) a telephone number is cited when the terminal is the cell phone. Furthermore, as another 'information unique to the terminal 100', it may be (2) an identifier that specifies the kind of the terminal 100 or an identifier different for each terminal such as a production number added to the terminal 100. In addition, there also exists a method of authenticating the TRM access library section 401 by using information regarding (3) a combination of the applications installed in the terminal 100. The 'applications installed in the terminal 100' means the application provided in the terminal, which is the application downloaded from outside the terminal 100 or the application stored in the ROM of the terminal 100. In this case, TRM access library section 401 outputs information to the authentication module 101 as to which application has been installed in the terminal 100 (the identifier of the installed application, for example), and the authentication module 101 performs authentication by determining whether or not the information that has been output matches the information stored in the tamper-resistant region. Alternatively, information of the invalid terminal information is stored in the tamper-resistant region, and the authentication module performs authentication by determining whether or not it does not match the invalid terminal information.

[0092] As an example of (3) cited above, it is assumed that a new service is provided for a person who is a member to receive both of service A and service B, for example. In this case, when TRM access library section 401 is authenticated by the authentication module 101 on condition that application A to receive service A and application B to receive service B are installed in the terminal 100, application C to receive service C can be provided for the member whose terminal has installed applications for service A and service B.

[0093] Further, there also exists a method of authenticating the TRM access library section 401 by using the information to identify the TRM access library section 401. The 'information to identify the TRM access library section 401' is information to identify software that constitutes the TRM access library section 401, for example, which is a name, a version or a serial number of the software. The TRM access library section 401 outputs the information to identify the TRM access library section 401 to the authentication module 101, and the authentication module 101 performs authentication by determining whether or not the information that has been output matches the information stored in the tamper-resistant region.

[0094] The 'processing for authentication of the application' is a processing for authentication of the application downloaded to the download section 102. The TRM access library section 401 may perform a part of the processing regarding authentication of the application. In addition, since the TRM access library section 401 has been authenticated by the authentication module 101, it may perform all the processing regarding authentication of the application.

[0095] Further, the processing performed by the TRM access library section 401 is not necessarily limited to the processing for application authentication. For example, as shown in Fig. 36, the TRM access library section 401 has an application manager and a device driver

therein, and may perform a processing for them.

[0096] The 'application manager' provides a function to control the application operation, such as startup, termination, and suspension. Note that an 'application control program' is cited as another name of the application manager, for example.

[0097] The 'device driver' is a program to control input/output with the authentication module. For example, it is a -program that absorbs specification of operation for input/output, which is different for each authentication module, and enables the application to perform input/output by an operation of a same interface. Note that an 'authentication module access program' is cited as another name of the device driver.

[0098] The TRM section 103 holds TRM access library section authentication information in the tamper-resistant region. The 'TRM access library section authentication information' is information to authenticate the TRM access library section 401. As already described, there are cases where this information is the information unique to the terminal 100 such as a cell phone number, the information regarding the combination of the applications installed in the terminal 100, or the information to identify the TRM access library section 401. Since the TRM access library section authentication information is held in the tamper-resistant region, there is also a case where the cell phone number, the information to identify the application installed in the terminal 100, and the information to identify the TRM access library section 401 are held in an encrypted form.

[0099] The TRM access library section authenticating section 402 authenticates the TRM access library section 401 of the terminal 100 based on the TRM access library section authentication information. Specifically, it performs authentication for the TRM access library section 401 with information for authentication output from the TRM access library section 401 to the authentication module 101 and the TRM access library section authentication information held in the TRM section 103.

[0100] Fig. 5 is a view for explaining a method of application authentication in the application authentication system in this embodiment. The difference between the application authentication systems shown in Figs. 4 and 5 is that the download section 102 of the terminal 100 in Fig. 5 downloads the application to which the signature, which is the information to authenticate that the application has not been tampered with, is added, the terminal 100 further has a signature authentication information output section 501, and the authentication module 101 further has a signature authentication information input section 502 and a signature authentication section 503.

[0101] The 'signature, which is the information to authenticate that the application has not been tampered with' is information to confirm that the application has not been tampered with. Fig. 6 shows a relationship between the application and the signature. An application main body 601 is qualified as data, a value obtained by applying the hash function such as SHA-1 and MD5 to the data is encrypted, and thus a signature 602 is formed. To confirm that the application main body has not been tampered with, by using the signature 602, the signature 602 is decrypted first to obtain the hash value. Next, the hash function is applied to the application main body to confirm whether or not a value obtained is the same as the hash value that is obtained by decrypting the signature 602. Alternatively, the hash function is applied to the application main body to obtain the hash value, it is encrypted, and determined whether or not the obtained value is the same as the signature 602. The former method is a method normally used when the signature 602 uses a public key cryptography, for example, where the signature 602 is generated by encrypting the hash value by a private key of a person who signs and is decrypted by a public key that corresponds to the private key of the person who has signed when confirmation is made that the application main body has not been tampered with. The latter method is used, for example, when a person who confirms that the application main body has not been tampered with knows the private key of the person who has signed, or when a symmetric key cryptography is used.

[0102] In this embodiment, TRM access library section 401, after having the authentication module 101 authenticate the section 401 itself, performs a processing that is a part of the processing for authentication of the application downloaded to the download section 102, that is, generating a digest for signature authentication from the application downloaded to the download section 102. The 'digest for signature authentication' is the hash value by the hash function such as SHA-1 and MD5.

[0103] The signature authentication information output section 501 outputs signature authentication information 506 generated in the TRM access library section 401, which includes a digest for signature authentication 504 and a signature 505, to authentication module 101. Herein, the 'signature 505' is a signature added to the application downloaded to the download section 102.

[0104] The signature authentication information input section 502 enters the signature authentication information 506 output from the signature authentication information output section 501.

[0105] The signature authentication section 503 performs verification for the signature based on the digest for signature authentication and the signature entered from the signature authentication information input section 502. As a method of verification, when the signature has been encrypted by the private key of the public key cryptography, for example, it is decrypted by the public key that corresponds to the private key and authentication is performed by comparing the result of the decryption and the digest for signature authentication to determine whether or not they are identical. Alternatively, there exists a method in which the symmetry key is held in the tamper-resistant region and the signature is de-

crypted by the symmetry key to compare with the digest for signature authentication, or a method in which the private key is held in the tamper-resistant region and the digest for signature authentication is encrypted by the private key to be compared with the signature.

[0106] Fig. 7 is the flowchart exemplifying the operation of the terminal 100. As a premise for performing the processing of the flowchart, it is assumed that the TRM access library section 401 has been authenticated by the authentication module 101. In step S701, the application is downloaded to the download section 102. In step S702, the TRM access library section 401 generates the digest for signature authentication by the downloaded application. In step S703, the signature authentication information output section 501 outputs the signature authentication information 506, which includes the digest for signature authentication found in step S702 and the signature added to the downloaded application, to the authentication module 101.

[0107] Fig. 8 is the flowchart explaining the operation of the signature authentication information input section 502 and the signature authentication section 503 of the authentication module 101. As a premise for performing the processing of the flowchart, it is assumed that the TRM access library section 401 has been authenticated by the authentication module 101. For this reason, there exists a method where it is assumed that the TRM access library section authenticating section 402 sets an authentication result in the authentication module 101, and in the case of performing the processing of the flowchart of Fig. 8, the authentication result that has been set is referred to and the processing of the flowchart of Fig. 8 is performed only when the TRM access library section 401 has been authenticated. In step S801, the signature authentication information input section 502 enters the signature authentication information 506. In step S802, verification for the signature is performed based on the digest for signature authentication 504 and the signature 505. The method of verifying the signature is as described above.

[0108] In this embodiment, since the TRM access library section 401, on condition that it has been authenticated by the authentication module 101, generates the digest for signature of the application downloaded to the download section 102, and the digest for signature authentication that has been generated is input to the authentication module 101, the digest for signature authentication is trustworthy and thus the authentication module 101 can perform authentication for the application downloaded to the download section 102.

Third Embodiment

[0109] Fig. 9 is the function block diagram of the authentication module 101 according to the third embodiment of the present invention. This embodiment shows the authentication method by the signature authentication information in the second embodiment more specifically, where the authentication module 101 of the second embodiment further has a signature-derived digest generation information obtaining section 901 and a signature-derived digest generation section 902.

[0110] The signature-derived digest generation information obtaining section 901 obtains signature-derived digest generation information for generating a signature-derived digest by using the signature entered from the signature authentication information input section 502. If the signature is the one in which the hash value of the application main body has been encrypted, the 'signature-derived digest generation information' is the decryption key that decrypts the encrypted value. When the public key cryptography is used as a method of encryption, the public key corresponding to the private key that has been used for encrypting the hash value of the application main body is the signature-derived digest generation information. The public key may be held in the authentication module 101. Further, it may be acquired from an appropriate server via the terminal 100 or the like.

[0111] The signature-derived digest generation section 902 generates a signature-derived digest 905 by using a signature 903 entered from the signature authentication information input section 502 and the signature-derived digest generation information held in the signature-derived digest generation information obtaining section 901. Specifically, if the signature-derived digest generation information is the public key, the public key decrypts the signature 903 to generate the signature-derived digest 905 that is the hash value of the application main body.

[0112] The signature authentication section 503 performs authentication based on the signature-derived digest 905 generated in the signature-derived digest generation section 902 and the digest for signature authentication entered from the signature authentication information input section 502. In other words, it compares the signature-derived digest 905 and the digest for signature authentication 904, authenticates the application downloaded to the download section 102 when they are the same, but does not authenticate it if they are different.

[0113] Fig. 10 is the flowchart explaining the operation of the signature authentication information input section 502, the signature-derived digest generation information obtaining section 901, the signature-derived digest generation section 902, and the signature authentication section 503 in this embodiment. As a premise for performing the processing of the flowchart, it is assumed that the TRM access library section 401 has been authenticated by the authentication module 101. For this reason, there exists a method where it is assumed that of the TRM access library section authenticating section 402 sets the authentication result in the authentication module 101, and in the case of performing the processing of the flowchart of Fig. 10, the authentication result that has been set is referred to and the processing of

the flowchart of Fig. 10 is performed only when the TRM access library section 401 has been authenticated. In step S1001, the signature authentication information input section 502 enters the signature authentication information 506 to obtain the signature 903 and the digest for signature authentication 904. In step S1002, the signature-derived digest generation information obtaining section 901 obtains the signature-derived digest generation information. In step S1003, the signature-derived digest 905 is generated in the signature-derived digest generation section 902 from the signature 903 and the signature-derived digest generation information. In step S1004, the signature authentication section 503 performs authentication based on the signature 903 and the digest for signature authentication 904.

Fourth Embodiment

[0114] Fig. 11 shows the function block diagram of the application authentication system in the fourth embodiment of the present invention. In this embodiment, the terminal of the application authentication system in the second embodiment or the third embodiment further has an authentication module authenticating section 1101.

[0115] The authentication module authenticating section 1101 authenticates the authentication module 101. As a method of this authentication, there exists the method shown by the flowchart shown in Fig. 12. In using the method, it is presumed that the private key of the public key cryptography and the public key corresponding to the private key are generated for the authentication module 101, and the authentication module 101 stores the private key therein. In step S1201, the authentication module authenticating section 1101 generates random numbers. In step S1202, the random numbers generated in step S1201 are encrypted by the public key that the authentication module 101 has. In step S1203, the random numbers encrypted in steps S1202 are input to the authentication module 101 to demand decryption. In step S1204, the authenticating section 1101 receives a decryption result from the authentication module 101, and it determines if the random numbers generated in step S1201 and the decryption result received in step S1204 are identical in step S1205. As another method, there exists a method where the authentication module authenticating section 1101 inputs the generated random numbers to the authentication module 101 and demand to encrypt the random numbers by the private key of the authentication module 101. The authentication module authenticating section 1101, having obtained the encryption result, decrypts it by the public key of the authentication module 101 and determines if it is identical to the random numbers input to the authentication module 101.

[0116] As described above, the terminal 100 can perform authentication for the authentication module 101 when the terminal 100 has the authentication module authenticating section 1101 for authenticating the authentication module 101. Thus, when the application operating in the terminal 100 writes highly confidential information (privacy information, log of E-commerce (EC), balance of an account in a banking transaction, or the like) in the authentication module 101, it is possible to confirm whether or not the authentication module 101 is the right one.

Fifth Embodiment

[0117] Fig. 13 shows the function block diagram of the application authentication system in the fifth embodiment of the present invention. This embodiment is a mode in which the TRM access library section 401 of the application authentication system in the fourth embodiment further has application-usable resource information holding means 1301.

[0118] The application-usable resource information holding means 1301 holds application-usable resource information. The 'application-usable resource information' is information regarding resources whose use is approved for an authenticated application. The 'authenticated application' is the application downloaded to the download section 102, to which the processing for authentication by the TRM access library section 401 has been performed and which has been authenticated correctly. The 'resources' are resources outside the application used by the application. The resources are: local resources that are resources of the terminal 100 and the authentication module 101 attached thereto; and other resources that are resources of the server, which is a communication destination of the terminal 100, for example. There exist several types of local resources such as use of memory, use of file, use of IrDA, use of Bluetooth, use of communication, use of TRM, use of application, and use of non-contact/contact IC card I/F. In addition, in the case of the use of memory among the local resources, there also exists one regarding a range of memory capacity and memory address. Furthermore, a range of usable time is cited as well.

[0119] Fig. 14 exemplifies the application-usable resource information. In Fig. 14, application-usable resource information 1400 is comprised of items such as use of memory 1401, use of file 1402, use of IrDA 1403, use of Bluetooth 1404, use of communication 1405, use of TRM 1406, use of application 1407, and use of non-contact/contact IC card I/F 1408, operation 1409, date and time of use 1410, and the like.

[0120] As items of the use of memory 1401, usable capacity as memory, address of a usable range, write-capable number, read-capable number, date and time when the memory can be used or cannot be used, and the like, are cited for example. Since writing is a loaded operation for a flash memory, restricting the number of writings to a memory is particularly meaningful.

[0121] As items of the use of file 1402, one that describes access restriction to a file that the terminal has or a file that an external memory such as the authenti-

cation module 101 connected to the terminal has, is cited. There exist, for example, an accessible directory name, an accessible file name, an accessible file type (specified by a file extension, for example), date and the time when the file can be or cannot be used, and the like.

[0122] The use of IrDA 1403 is an item showing whether or not the use of an infrared communication function, which the terminal has, is approved, and time when the function can/cannot be used, total usable time, the number of uses, and the like are cited.

[0123] The use of Bluetooth 1404 is an item showing whether or not the use of a communication function via Bluetooth is approved, and intensity of radio waves where the function can be used, the number of roaming, date and time when it can/cannot be used are cited other than the time when the function can be used, total usable time, the number of uses, and the like. By specifying the intensity of radio waves where the function can be used, a distance from which communication is possible can be specified.

[0124] The use of communication 1405 is an item showing whether or not the use of a communication function with the server or the like is approved, and an accessible server or the like is cited other than the time when the function can/cannot be used, total usable time, the number of uses, intensity of radio waves where it can be used, and the number of roaming. The server accessible by the application is specified by an IP address, a domain name, a server function such as a mail server and an FTP server, or communication protocol with a server.

[0125] The use of TRM 1406 is an item showing whether or not access to the tamper-resistant region of the authentication module 101 or the like is approved, which is the date and time when access to the tamper-resistant region can or cannot be made, the number of accesses, or a card application that operates in an IC card having the tamper-resistant region, and an accessible card application, types of usable IC card commands, and the like are cited.

[0126] The use of application 1407 is an item where the application specifies another linkable application. For example, it is an address book, e-mail, scheduler, game, or the like. In addition, the date and time when link is possible with another application may be included. When the terminal 100 is a cell phone, whether or not the application is approved to operate in parallel with a call during telephone communication, or whether or not it must be stopped or finished when the call starts may be specified.

[0127] The use of contact/non-contact IC card I/F 1408 is an item showing whether or not the use of an interface for communicating with a contact/non-contact IC card or an IC card rewriter, which is capable of communicating with the terminal 100, is approved. The time when the interface can be used, total usable time, the number of usable/non-usable times, a usable I/F (type A, type B, type C, or the like), a type of usable IC card command, and the like are cited.

[0128] The date and time of use 1410 specifies date and time when the application can operate. Alternatively, it specifies date and time when the operation of the application should stop.

[0129] When the application downloaded to the download section 102 uses the resources, it sends a demand to use resources to the TRM access library section 401. The TRM access library section 401 refers to the application-usable resource information held in the application-usable resource information holding means 1301 and determines whether or not the demanded resource can be used, and it allows the application to use the demanded resource if it is usable.

[0130] The application-usable resource information is downloaded to the download section 102 together with the application to be downloaded, and it may be held in the application-usable resource information holding means 1301.

Fig. 15 is the view schematically showing data where the application-usable resource information is downloaded together with the application. Firstly, there exists application data 1501 that is the application main body followed by application data signature data 1502 that is a signature for authenticating the application data 1501, and there further exist application-usable resource information 1503 and application-usable resource information signature data 1504 for authenticating the application-usable resource information. In the application-usable resource information 1503, an expression such as 'IrDA 1' (IrDA is usable) and 'Bluetooth 0' (Bluetooth is not usable) is shown like an area added with reference numeral 1505.

[0131] Further, the application-usable resource information is stored in the authentication module 101, read out if necessary, and may be held in the application-usable resource information holding means 1301.

[0132] As described above, with a configuration in which the TRM access library section 401 has the application-usable resource information holding means 1301, the downloaded application can restrict usable resources. Accordingly, a user can conduct business in which he/she issues the application-usable resource information to a producer of the application or a service provider to receive a counter value. The application-usable resource information can be used for approval control of the local resource, and approval/disapproval of the use of the local resource can be finely set for a particular application. In the case of approving the use of local resources, business transaction by issuing the application-usable resource information is made possible when the user pays use fees to an issuer of the application-usable resource information. Furthermore, the user of the terminal 100, by paying the counter value, can obtain the application-usable resource information of the downloaded application, which is less restricted for the use of the resource, and thus business transaction where the user of the terminal 100 is a customer

can be realized.

[0133] Note that, in the second to fifth embodiment, the download section 102 may download a use license. The 'use license' is the application-usable resource information added with the signature of a downloaded application. The 'downloaded application' is the application downloaded to the download section 102. The 'application-usable resource information added with the signature' is the application-usable resource information to which the signature of the application-usable resource information has been added. Since the application-usable resource information is a license for the downloaded application to use the resources of the terminal 100 or the authentication module 101, it is important to guarantee authenticity of the application-usable resource information. For this reason, the signature is added to the application-usable resource information.

[0134] Note that verification of the signature of the downloaded application and verification of the signature of the application-usable resource information may be performed either simultaneously or at different occasions. For example, if the application is verified first, verification of the signature of the application-usable resource information is performed to confirm that the signature is authentic when the application has started operation and accessed to the resources, and whether or not access to the resource is approved may be determined. In addition, creators of the signature of the downloaded application and the signature of the application-usable resource information may be the same or different. The reason why the creators of the signatures may be different is that there are cases where the creator of the application, and the issuer of the application-usable resource information are different and the former applies to the latter for approval of the use of the resources and receives issuance of the application-usable resource information from the latter. Note that the counter value may be paid at the time of application for approval of the use of the resources.

[0135] Furthermore, in the case where the application-usable resource information of the use license includes expiry date information showing a time limit for accessing to the resources, the download section 102 downloads the use license and may update the use license when time information approved based, on the expiry date information, has already expired.

[0136] Still further, the use license may be downloaded at the time of executing the downloaded application and/or authenticating the application. The use license may be downloaded from the server with which the terminal 100 can communicate. It may be downloaded from the authentication module 101 as well.

[0137] Although it is possible that the download section 102 continues to hold the use license downloaded from the server, there are cases in which the use license has been updated in the server and thus the use license held in the download section 102 may have expired. Therefore, the download section 102 may inquire to the server of the validity of the downloaded use license at the time of executing the downloaded application and/or authenticating the application.

[0138] In the download section 102, the download section 102 or another section of the terminal 100 inquires to the server of the contents of the use license (via on-line), and it may inquire whether or not the use of the resource of the application has been approved.

Sixth Embodiment

[0139] Fig. 16 shows the function block diagram of the application authentication system in the sixth embodiment of the present invention. In this embodiment, the TRM access library section 401 of the terminal 100 of the application authentication system in the fourth embodiment or the fifth embodiment further has application-usable resource information output means 1601.

[0140] The application-usable resource information output means 1601 outputs the application-usable resource information to the authentication module 101 that has been authenticated by the authentication module authenticating section 1101.

[0141] In this embodiment, the TRM section 103 of the authentication module 101 holds the application-usable resource information, which has been output from the application-usable resource information output means 1601, in the tamper-resistant region in a rewritable manner.

[0142] The application-usable resource information held in the tamper-resistant region is read into the terminal 100 if necessary, and referred to in order to determine whether or not resources are usable when the application downloaded to the download section 102 uses the resources.

[0143] As described above, the TRM access library section 401 has the application-usable resource information output means 1601 and the TRM section 103 holds the application-usable resource information output from the application-usable resource information output means 1601, by which the application-usable resource information can be rewritten, if necessary, even after the application-usable resource information has been provided in the state where it is held in the authentication module 101. For example, rewriting of the expiry date of the application-usable resource information can be done. Further, by payment of the counter value from the service provider or the service user, the application-usable resource information held in the tamper-resistant region can be updated to one, which is less restricted for the usable resource of the application, for example. Because the TRM access library section 401, which has been authenticated by the signature authentication information input section 502 in advance, performs rewriting, invalid rewriting can be prevented.

Seventh Embodiment

[0144] Fig. 17 shows the function block diagram of the application authentication system in the seventh embodiment of the present invention. In this embodiment, the terminal 100 of the application authentication system in the fifth embodiment or the sixth embodiment further has an application-usable resource information download section 1701.

[0145] The application-usable resource information download section 1701 downloads application-usable resource information 1702 added with a signature 1703. This information may be downloaded together with the application downloaded to the download section 102 as shown in Fig. 15. On the other hand, it may be downloaded in addition to the application downloaded to the download section 102. For example, the application is previously downloaded, and the application-usable resource information 1702 may be downloaded when the application makes access to the resource.

[0146] In this embodiment, the TRM access library section 401 may authenticate the signature 1703 added to the application-usable resource information 1702 that has been downloaded to the application-usable resource information download section 1701. Since the authentication module 101 authenticates the TRM access library section 401, a result that the TRM access library section 401 has correctly authenticated the signature 1703 of the application-usable resource information 1702 is trustworthy for the authentication module 101. Therefore, it is guaranteed that an invalid operation does not occur even if the downloaded application accesses to the authentication module 101 according to the application-usable resource information 1702 authenticated in this manner.

Eighth Embodiment

[0147] Fig. 18 shows the function block diagram of the application authentication system in the eighth embodiment of the present invention. In this embodiment, the terminal 100 of the application authentication system in the fifth embodiment or the sixth embodiment has the application-usable resource information download section 1701 and a signature authentication information output section for application-usable resource information 1801, and the authentication module 101 has a signature authentication information input section for application-usable resource information 1802 and a signature authentication section for application-usable resource information 1803. This embodiment is a mode in which the authentication module 101 authenticates the signature 1703 instead of the seventh embodiment where the TRM access library section 401 authenticates the signature 1703 added to the application-usable resource information 1702.

[0148] The application-usable resource information download section 1701 downloads the application-usable resource information 1702 added with the signature 1703.

[0149] In this embodiment, the TRM access library section 401 generates the digest for signature authentication from the application-usable resource information 1702 that has been downloaded to the application-usable resource information download section 1701, and the signature authentication information output section for application-usable resource information 1801 outputs signature authentication information 1806, which includes the digest for signature authentication generated and the signature 1703, to the authentication module 101.

[0150] The signature authentication information input section for application-usable resource information 1802 enters the signature authentication information 1806 that has been output from the signature authentication information output section for application-usable resource information 1801. The signature authentication information 1806 includes a digest for signature authentication 1804 generated in the TRM access library section 401 and a signature 1805 that is the signature 1703 added to the application-usable resource information 1702.

[0151] The signature authentication section for application-usable resource information 1803 performs verification for the signature based on the digest for signature authentication 1804 and the signature 1805, which are entered from the signature authentication information input section for application-usable resource information 1802.

[0152] Fig. 19 is the flowchart explaining the operation of the terminal 100 in this embodiment. In step S1901, the TRM access library section 401 generates the digest for signature authentication 1804 from the application-usable resource information 1702. In step S1902, the signature authentication information output section for application-usable resource information 1801 outputs the signature authentication information 1806, which includes the digest for signature authentication 1804 and the signature 1805, to the authentication module 101. In step S1903, the terminal receives the authentication result from the authentication module 101.

[0153] Fig. 20 is the flowchart explaining the operation of the authentication module 101 in this embodiment. In step S2001, the signature authentication information input section for application-usable resource information 1802 enters the signature authentication information 1806. In step S2002, the signature authentication section for application-usable resource information 1803 performs verification of the signature 1805 based on the digest for signature authentication 1804 and the signature 1805. In step S2003, the module returns a verification result to the terminal 100.

[0154] In the above-described embodiment, since the signature of the application-usable resource information 1702 is authenticated based on the digest for signature authentication generated by the TRM access library

section 401 that has been authenticated by the authentication module 101, the authentication result is trustworthy. Further, since it is possible that authentication in the signature authentication section for application-usable resource information 1803 is performed, not based on encryption but by determining whether or not a signature matches the signature stored in the TRM section of the authentication module 101, authentication can be performed with a simple task.

Ninth Embodiment

[0155] The ninth embodiment of the present invention is characterized in an in-authentication-module application, which operates in the authentication module 101, accepts access from the application operating in the terminal 100 on condition that the TRM access library section 401 has been authenticated by the authentication module 101.

[0156] Fig. 21 shows the function block diagram of the application authentication system in this embodiment. In this embodiment, the terminal 100 of the application authentication system in the second embodiment and the third embodiment has a terminal application holding section 2101, and the authentication module 101 has the TRM section 103 provided with an in-authentication-module application holding section 2103.

[0157] The terminal application holding section 2101 holds a terminal application 2102 that accesses the TRM section of the authentication module 101. The 'terminal application 2102' is an application executed inside the terminal 100. The application may be the application downloaded by the download section 102, or may be the application held in the ROM of the terminal 100. To 'hold' means to make the terminal application 2102 executable. Therefore, the terminal application holding section 2101 is realized by a rewritable memory region of the terminal 100, where all or a part of the terminal application 2102 is loaded, to execute the terminal application 2102.

[0158] The in-authentication-module application holding section 2103 holds an in-authentication-module application 2104. The 'in-authentication-module application 2104' is an application that operates in the authentication module 101. If the authentication module 101 is an IC card, in-authentication-module application 2104 is the card application. To 'hold' means to make the in-authentication-module application 2104 executable. Therefore, the in-authentication-module application holding section 2103 is realized by a rewritable memory region of the authentication module 101, where all or a part of the in-authentication-module application 2104 is loaded, to execute the in-authentication-module application 2104.

[0159] In this embodiment, the in-authentication-module application 2104 operates on accepting access from the terminal application 2102 on condition that the TRM access library section authenticating section 402 authenticates the TRM access library section 401. For this reason, a value showing whether or not the TRM access library section 401 has been authenticated is stored in the authentication module 101, and, as shown in Fig. 22, the authentication module checks if the value itself or a similar value exists and determines whether or not authentication of the TRM access library section 401 has succeeded in step 2201. If authentication has succeeded, the processing proceeds to step S2202, and the application 2104 accepts access from the terminal application 2102. The determination in step S2201 is performed either in the in-authentication-module application 2104 or in a section other than the in-authentication-module application 2104. When it is performed in the in-authentication-module application 2104, determination is made by checking with the value, which shows whether or not the TRM access library section 401 has been authenticated, during the time when the in-authentication-module application 2104 is activated until the time when the terminal application 2102 accesses the application 2104. When the determination of step S2201 is performed in a section other than the in-authentication-module application 2104, the value showing whether or not the TRM access library section 401 has been authenticated is confirmed at the time when the in-authentication-module application 2104 is activated.

[0160] Since a card manager activates the in-authentication-module application 2104 when the authentication module 101 is an IC card, the card manager checks with the value, which shows whether or not the TRM access library section 401 has been authenticated, and determines if it activates the in-authentication-module application 2104. Furthermore, in deciding whether or not an interface section (not shown in Fig. 21) for the authentication module 101 approves access from the terminal application 2102 to the in-authentication-module application 2104, determination may be made by checking with the value, which shows whether or not the TRM access library section 401 has been authenticated.

[0161] Further, the in-authentication-module application 2104, every time it receives access from the terminal application 2102, checks with the value showing whether or not the TRM access library section 401 has been authenticated and may decide if it operates on accepting the access. Fig. 23 is the flowchart explaining the operation of the in-authentication-module application 2104 in such a case. In step S2301, the in-authentication-module application 2104 receives access from the terminal application 2102. In step S2302, the in-authentication-module application 2104 checks with the value showing whether or not the TRM access library section 401 has been authenticated and determines if authentication of the TRM access library section 401 has succeeded. If the authentication has succeeded, the application 2104 operates on accepting access from the terminal application 2102 in step S2303.

[0162] Fig. 24 shows a mode where the value show-

ing whether or not the TRM access library section 401 has been authenticated is stored in the TRM section 103. The TRM section 103 has authentication result identifier generating means 2401. The authentication result identifier generating means 2401 generates an authentication result identifier 2402 on condition that authentication of the TRM access library section 401 by the TRM access library section authenticating section 402 succeeds. The in-authentication-module application 2104 accepts access from the terminal application 2102 on condition that the authentication result identifier 2402 exists.

[0163] Note that the authentication result identifier 2402 does not only indicate authentication success of the TRM access library section 401 by the TRM access library section authenticating section 402, but also may have contents indicating authentication failure. In this case, the authentication result identifier generating means 2401 generates the authentication result identifier 2402 that has contents according to authentication success/failure of the TRM access library section 401 by the TRM access library section authenticating section 402. Further, the in-authentication-module application 2104 checks with the contents of the authentication result identifier 2402 and determines whether or not authentication has succeeded.

[0164] Fig. 25 shows a method of realizing the authentication result identifier 2402 when the authentication module 101 is an IC card. In Fig. 25, card application A (2501) authenticates the TRM access library section 401, and it sets the authentication result identifier 2402 in the rewritable memory region, which is a RAM region 2503 for example, when the TRM access library section 401 has been authenticated. In Fig. 25, a flag sign schematically expresses the authentication result identifier 2402. The card application A (2501) can read/write in the RAM region 2503, but another card application B (2502) cannot access to the RAM region 2503 directly due to a firewall function that activates each application independently, so that applications in the IC card do not adversely effect each other. Then, the card application A (2501), using a sharable interface function where the interface can be shared on specifying a destination, provides a sharable interface 2504. The card application B (2502), to which the terminal application 2402 has accessed, confirms whether or not the authentication result identifier 2402 exists in the RAM region 2503 through the sharable interface 2504.

[0165] Further, Fig. 26 shows another method of realizing the authentication result identifier 2402 when the authentication module 101 is an IC card. Rectangles added with reference numerals 2601 and 2602 express dedicated files (DF). Each DF corresponds to each card application. Accordingly, when the DF is selected, the card application corresponding to the DF is activated. Hereinafter, DF with reference numeral 2601 and DF with reference numeral 2602 correspond to application A and application B, respectively. Rectangles added with reference numerals 2603, 2604, 2605, 2606 and 2607 express elementary files (EF). When a card application corresponding to DF is activated, EF directly under DF can be operated. For example, when DF with reference numeral 2601 is selected and card application A is activated, card application A becomes capable of accessing EF with reference numerals 2603 and 2604.

[0166] Hereinafter, it is presumed that the authentication result identifier 2402 is set to EF with reference numeral 2604 when card application A has performed authentication and has correctly authenticated the TRM access library section 401. When a security status of DF added with reference numeral 2601 includes a state of EF added with reference numeral 2604, selection of DF, which corresponds to offspring of DF added with reference numeral 2601 in a tree structure formed by DF and EF, can be controlled. Specifically, in the selection of DF with reference numeral 2602, setting is made on condition that the identifier in either one of the offspring of DF added with reference numeral 2601, which is EF added with reference numeral 2604, in this case, exists. In other words, since selection of DF corresponding to card application B can be controlled due to the authentication result of the TRM access library section 401 by card application A, card application B can be activated only when the TRM access library section 401 has been authenticated.

[0167] As a result of this embodiment, security of the authentication module 101 is maintained because the in-authentication-module application 2104 has never been accessed from the terminal application 2102 unless the TRM access library section 401 is authenticated by the authentication module 101.

[0168] Note that the in-authentication-module application holding section 2103 may be outside the TRM section 103. In this case, the in-authentication-module application 2104 checks whether or not the TRM access library section authenticating section 402 has authenticated the TRM access library section 401, and operates on accepting access from the terminal application 2102.

Tenth Embodiment

[0169] Fig. 27 shows the function block diagram of the application authentication system in the tenth embodiment of the present invention. In the tenth embodiment of the present invention, in-authentication-module application 2104 operates on accepting access from the application operating in the terminal 100 on condition that the application has been authenticated. The application authentication system in this embodiment is a mode in which the TRM section 103 of the application authentication system in the ninth embodiment has application authentication result identifier generating means 2701.

[0170] The application authentication result identifier generating means 2701 generates an application authentication result identifier 2702 on condition that ap-

plication authentication by the TRM access library section 401 has succeeded. Herein, the 'application' is the application downloaded to the download section 102. The 'application authentication by the TRM access library section 401' means authentication performed based on the signature added to the application and the digest for signature authentication.

[0171] In this embodiment, the in-authentication-module application 2104 enables the terminal application 2102 to access to the in-authentication-module application 2104 on condition that the application authentication result identifier 2702 showing success of authentication exists, and the in-authentication-module application 2104 accepts access from the terminal application 2102.

[0172] For example, in the case where the terminal application 2102 has already been operating first and the in-authentication-module application 2104 has not operated yet, the in-authentication-module application 2104 is activated only when the application authentication result identifier 2702 exists, in activating the in-authentication-module application 2104. Alternatively, in the case where both of the terminal application 2102 and the in-authentication-module application 2104 have been activated, when access has occurred from the terminal application 2102 to the in-authentication-module application 2104, it accepts the access only when the application authentication result identifier 2702 exists.

[0173] If only one terminal application that accesses to the in-authentication-module application 2104 operates in the terminal 100, one kind of the application authentication result identifier 2702 is enough. However, if a plurality of such terminal applications operate in the terminal 100, the application authentication result identifier generating means 2701 generates the application authentication result identifier 2702 for every terminal application in order to show which terminal application has been authenticated. Alternatively, when it is guaranteed that two or more terminal applications do not access to the in-authentication-module application 2104 simultaneously, only one kind of the application authentication result identifier 2701 is generated. Accordingly, the application authentication result identifier 2702 is generated only at the moment when the authenticated terminal application accesses to the in-authentication-module application 2104, and the application authentication result identifier 2702 may be deleted when access by the authenticated terminal application to the in-authentication-module application 2104 ends.

[0174] Due to this embodiment, only the terminal application 2102 that has been authenticated can access to the in-authentication-module application 2104, and thus the security of the authentication module 101 is assured.

Eleventh Embodiment

[0175] Fig. 28 shows the function block diagram of the application authentication system in the eleventh embodiment of the present invention. The application authentication system in this embodiment is comprised of the terminal, the authentication module, and the server that downloads the application to the terminal.

[0176] In Fig. 28, a terminal 2801 has a download section 2804. The download section 2804 is a section to download the application. For example, it downloads the application from a server 2803.

[0177] The authentication module 2802 has a TRM section 2805. The TRM section 2805 holds information for processing application authentication in the tamper-resistant region. Herein, the 'application' means the application downloaded to the download section 2804 of the terminal 2801. The 'application authentication' means to confirm that the application does not perform invalid operation such as whether or not the application has been issued by a credible person, has been guaranteed not to perform invalid operation, or has been tampered with after it was issued by the credible person or has been tampered with after it was guaranteed not to operate obliquely. As a method of processing the authentication, the hash function such as the SHA-1 and the MD5, where finding two different input data such that the resultant data obtained after processing the input data match is difficult, is generally used in order to find the resultant data obtained by processing the data for executing the application as input data, and the data encrypted (a so-called 'signature') is used. Therefore, the 'information for processing the application authentication' is the actual signature or the decryption key necessary for decrypting the signature to obtain the hash value. The 'tamper-resistant region' is a storage area of the authentication module 2802, which is a storage area whose data is difficult to read out or rewrite in an invalid manner. For example, to access to the storage area, the user must go through hardware that is not accessible unless the user takes the right procedure to access the storage area, or that the data stored in the storage area is encrypted.

[0178] The server 2803 has a terminal authentication section 2806. The terminal authentication section 2806 determines that authentication of the terminal 2801 has succeeded on condition that authentication for the authentication module 2802 via the terminal 2801 succeeds. Specifically, the server 2803 performs authentication for the authentication module 2802. During authentication, the server 2803 and the authentication module 2802 need to communicate with each other and the communication is performed by relaying the terminal 2801. As a method where the server 2803 performs authentication for the authentication module 2802, the server 2803 generates the random numbers, encrypts the random numbers by the public key of the authentication module 2802, and demands the authentication module 2802 via the terminal to decrypt the encrypted random numbers. The authentication module 2802 obtains the random numbers generated by the server 2803

through decryption using the private key, which is stored in the tamper-resistant region, of the authentication module 2802, and returns it to the server 2803 by relaying the terminal 2801. The server 2803 determines whether or not the generated random numbers and the random numbers sent from the authentication module 2802 are identical and performs authentication. Alternatively, there also exists a method where the server 2803 directly sends the random numbers to the authentication module 2802, the authentication module 2802 encrypts them by the private key to return the result to the server 2803, and the server 2803 decrypts the result by the public key of the authentication module 2802, and performs authentication for the authentication module 2802 by determining whether or not the decrypted random numbers are identical to the random numbers sent to the authentication module 2802.

[0179] Since the authentication module 2802 is attached to the terminal 2801, the terminal 2801 to which the authentication module 2802 has been attached is authenticated as well when the server 2803 authenticates the authentication module 2802. Additionally, authentication is further assured when the authentication module 2802 authenticates the terminal 2801 on condition that unique information, which the terminal 2801 has, such as a production number of the terminal 2801, an identifier showing a unit type, an identifier stored in the ROM of the terminal 2801, and a version number, exists in tamper-resistant region.

[0180] This enables the server 2803 to perform authentication for the terminal 2801 even without the tamper-resistant region in the terminal 2801, and the server can correctly authenticate the terminal 2801. Thus, an accounting processing, a settlement processing or the like can be performed between the server 2803 and the terminal 2801. Furthermore, the server 2803 can download the application including highly confidential data to the terminal 2801, and thus the application authentication system in this embodiment can execute a complicated business transaction operation.

Twelfth Embodiment

[0181] Fig. 29 shows the function block diagram of the application authentication system according to the twelfth embodiment of the present invention. In this embodiment, the application authentication system is comprised of the terminal 2801, authentication module 2802, and the server 2803 that downloads the application to the terminal 2801, as shown in the eleventh embodiment.

[0182] The terminal 2801 has the download section 2804 and a TRM access library section 2901. The download section 2804 downloads the application. In this case, the application is downloaded from the server 2803. Alternatively, it may be downloaded from a section other than the server 2803. The TRM access library section 2901 performs processing for application authentication on condition that the authentication module 2802 authenticates the section 2901 itself. Specifically, the TRM access library section 2901 makes the authentication module 2802 authenticate the section 2901 itself, and when it is authenticated correctly, it performs processing for authenticating the application downloaded to the download section 2804. As a method that the TRM access library section 2901 makes the authentication module 2802 authenticate the section 2901 itself, there exists a method where information unique to the terminal 2801 such as a production number, an identifier showing a terminal type, or a serial number or a version number of software, which realize the TRM access library section 2901, for example, is output to the authentication module 2802 to check whether or not the unique information of the terminal 2801, the serial number, the version number or the like, which has been output to the tamper-resistant region, exists.

[0183] The authentication module 2802 has the TRM section 2805 and a TRM access library section authenticating section 2902. The TRM section 2805 holds the TRM access library section authentication information, which is information for authenticating the TRM access library section 2901, in the tamper-resistant region. As the 'TRM access library section authentication information', the information unique to the terminal 2801 such as the production number, the identifier showing the terminal type, or the serial number or the version number of software, which realize the TRM access library section 2901, for example, is cited as described above. The TRM access library section authenticating section 2902 authenticates the TRM access library section 2901 of the terminal 2801 based on the TRM access library section authenticating section information. As a method of the authentication, there exists a method where the TRM access library section authenticating section 2902 receives identification information such as the information unique to the terminal 2801 that has been output from the TRM access library section 2901, or the serial number and the version number in the TRM access library section 2901, and checks whether or not the identification information exists in the TRM section 2805, as described above. The result of authentication is output from the TRM access library section authenticating section 2902 to the TRM access library section 2901. Further, the result of authentication is held in the authentication module 2802, and referred to in the case of exchanging information with the terminal 2801 later. Then, the authentication module 2802 exchanges correct information when the TRM access library section 2901 has been correctly authenticated, or exchanges incorrect information if the section 2901 has not been correctly authenticated.

[0184] The server 2803 has a server TRM access library section authenticating section 2903. The server TRM access library section authenticating section 2903 determines that authentication for the TRM access library section 2901 has succeeded on condition that au-

thentication of the TRM section 2805 in the authentication module 2802 via the TRM access library section 2901 of the terminal 2801 succeeds. The following is a method that the server TRM access library section authenticating section 2903 performs authentication for the TRM section 2805 in the authentication module 2802 via the TRM access library section 2901 of the terminal 2801. Specifically, the server 2803 generates random numbers, encrypts the random numbers by the public key of the authentication module 3802, and demands the authentication module 2802 via the terminal 2801 to decrypt the encrypted random numbers. The authentication module 2802 decrypts the random numbers using its private key stored in the tamper-resistant region, and returns them to the server 2803 via the terminal 2801. The server 2803 determines whether or not the random numbers generated and the random numbers sent from the authentication module 2802 are identical to perform authentication. Alternatively, there also exists a method that the server 2803 sends the random numbers directly to the authentication module 2802, the authentication module 2802 encrypts them by its private key to return the result to the server 2803, the server 2803 decrypts it by the public key of the authentication module 2802, and authenticates the authentication module 2802 by determining whether or not the decrypted numbers are identical to the random numbers sent to the authentication module 2802.

[0185] Fig. 30 is the sequence diagram explaining the interaction among the server TRM access library section authenticating section 2903, the TRM access library section 2901, and the authentication module 2802. In step S3001, the TRM access library section 2901 outputs a demand to authenticate itself to the authentication module 2802, and an authentication result in the authentication module 2802 is output in step S3002. In step S3003, the server TRM access library section authenticating section 2903 outputs an authentication demand to the TRM access library section 2901, and in response to this, the TRM access library section 2901 outputs the authentication demand to the authentication module 2802 in step S3004, and the authentication module 2802 returns the result such that the module itself is authenticated by the server TRM access library section authenticating section 2903, in step S3005. At this point, it returns either a correct result or an incorrect result depending on whether or not the TRM access library section 2901 has been authenticated correctly. In step S3006, the TRM access library section 2901 returns the result output from the authentication module 2802 to the server TRM access library section authenticating section 2903. The server TRM access library section authenticating section 2903 checks with the result, and determines that the TRM access library section 2901 has been authenticated as well when it can authenticate the authentication module 2802.

[0186] As described above, the result of authentication for the TRM access library section 2901 by the server TRM access library section authenticating section 2903 is held inside the authentication module 2802, and the authentication module 2802 either performs or does not perform exchange of the correct information according to the authentication result. Therefore, when the server 2803 performs authentication for the TRM section in the authentication module 2802 via the TRM access library section 2901, and if it can correctly authenticate it, it may be determined that authentication for the TRM access library section 2901 has succeeded.

[0187] With this procedure, the server 2803 can perform authentication for the terminal 2801 even if the terminal 2801 does not have the tamper-resistant region, the server 2803 can correctly authenticate the terminal 2801, and thus an accounting processing, a settlement processing or the like can be performed between the server 2803 and the terminal 2801. Furthermore, the server 2803 can download the application including highly confidential data to the terminal 2801, and thus the application authentication system in this embodiment can execute a complicated business transaction operation.

[0188] Further, when the TRM access library section authenticating section 2902 authenticates the TRM access library section 2901, the authentication module 2802 determines that the TRM access library section 2901 is trustworthy. Thus, when the TRM access library section 2901 performs all or a part of authentication processing of the application downloaded to the download section 2804, the result of all or a part of authentication processing of the application performed by the TRM access library section 2901 is trustworthy for the authentication module 2802. Therefore, the authentication module 2802 can perform authentication for the application downloaded to the download section 2804 by using the result of all or a part of authentication processing of the application by the TRM access library section 2901. As a result, access to data inside the authentication module 2802 can be permitted to the application that has been correctly authenticated, and a complicated business transaction can be performed.

[0189] Note that the processing for application authentication by the TRM access library section 2901 may be performed on condition that the application has accessed the tamper-resistant region of the TRM section 2805 in the authentication module 2802. This eliminates a need to perform authentication for an application that does not access to the tamper-resistant region.

[0190] Further, the TRM access library section 2901 may perform the processing for application authentication on condition that the application has been downloaded to the download section 2804. With this processing, authentication for all downloaded applications is performed and there will be no possibility that the terminal 2801 executes an invalid application.

[0191] Still further, the TRM access library section 2901 may perform the processing for application authentication while using the start of application execu-

tion as a trigger. This makes it possible to omit authentication for an application that has been downloaded but not been executed.

Thirteenth Embodiment

[0192] Fig. 31 shows the function block diagram of the application authentication system in the thirteenth embodiment of the present invention. The application authentication system according to this embodiment comprises the terminal 2801, the authentication module 2802, and the server 2803 that downloads the application to the terminal 2801.

[0193] The terminal 2801 has the download section 2804 and the TRM access library section 2901, and the TRM access library section 2901 includes a digest for signature generating means 3101, downloaded application signature obtaining means 3102, and application authentication data output means 3103.

[0194] The download section 2804 downloads an application 3104. The application 3104 may be downloaded from the server 2803. It also may be downloaded from a section other than the server 2803, that is, the authentication module 2802, for example. In this embodiment, the application 3104 is downloaded along with a signature 3105 of the application 3104. 'Downloaded along with the signature 3105' does not only mean that they are downloaded simultaneously but also mean that the application 3104 may be downloaded before or after downloading the signature 3105. In other words, it means that the application 3104 and the signature 3105 are downloaded by the time when authentication for the application 3104 (described later) is performed.

[0195] The digest for signature generating means 3101 generates digest for signature from the application 3104. Specifically, it generates the digest for signature from the application 3104 downloaded to the download section 2804. The 'digest for signature' is a value obtained using the same hash function as the one used in generating the signature 3105.

[0196] The downloaded application signature obtaining means 3102 obtains the signature 3105 that has been downloaded along with download of the application 3104. As described above, 'downloaded along with download of the application 3104' does not only mean that they have been downloaded simultaneously, but it also means that the application 3104 and the signature 3105 are downloaded by the time when authentication for the application 3104 (described later) is performed.

[0197] The application authentication data output means 3103 transmits the obtained signature and the digest for signature generated by the digest for signature generating means 3101 to the server 2803. The 'obtained signature' is the signature 3105 obtained by the downloaded application signature obtaining means 3102.

[0198] The digest for signature generating means 3101, the downloaded application signature obtaining means 3102, and the application authentication data output means 3103 perform a processing for authenticating the application 3104 downloaded to the download section 2804. This processing may be performed on condition that the authentication module 2802 has authenticated the TRM access library section 2901.

[0199] The authentication module 2802 has the TRM section 2805 and the TRM access library section authenticating section 2902. The TRM section 2805 and the TRM access library section authenticating section 2902 are sections identical to the TRM section and the TRM access library section authenticating section in the twelfth embodiment.

[0200] The server 2803 has the server TRM access library section authenticating section 2903, an application authentication data input section 3106, and a server application authenticating section 3107.

[0201] The server TRM access library section authenticating section 2903 is identical to the one in the twelfth embodiment, and it determines that authentication of the TRM access library section 2901 has succeeded on condition that authentication of the TRM section 2805 in the authentication module 2802 via the TRM access library section 2901 of the terminal 2801 succeeds.

[0202] The application authentication data input section 3106 enters the digest for signature and the signature, which have been output from the application authentication data output means 3103 of the TRM access library section 2901 whose authentication has been determined as successful by the server TRM access library section authenticating section 2903.

[0203] The server application authenticating section 3107 performs authentication for the application 3104 based on the digest for signature and the signature, which have been input to the application authentication data input section 3106. Authentication is performed in such a manner that the signature is decrypted to find the digest and whether or not the digest is identical to the digest for signature is determined. If the signature has been encrypted by the private key of the server 2803 in the public key cryptography, the private key of the server 2803 encrypts the digest for signature input to the application authentication data input section 3106, and authentication may be determined based on whether or not the signature obtained is identical to the signature input to the application authentication data input section 3106.

[0204] Fig. 32 shows the interaction along the passage of time among the server 2803, the terminal 2801, and the authentication module 2802, which constitute the application authentication system in this embodiment. Steps from S3201 to S3206 are the same as steps from S3001 to S3006 in Fig. 30 of the twelfth embodiment. When the application 3104 is downloaded to the download section 2804 after step S3206, the digest for signature generating means 3101 generates the digest for signature of the application 3104, the downloaded

application signature obtaining means 3102 obtains the signature 3105, and the application authentication data output means 3103 outputs the digest for signature and the signature 3105 to the application authentication data input section 3106 (step S3207). Then, the server application authenticating section 3107 performs authentication for the application 3104 by the digest for signature and the signature, which have been input to the application authentication data input section 3106.

[0205] According to this embodiment, the server TRM access library section authenticating section 2903 in the server 2803 determines that authentication for the TRM access library section 2901 in the terminal 2801 has succeeded on condition that authentication for the TRM section 2805 in the authentication module 2802 via the TRM access library section 2901 of the terminal 2801 succeeds. Accordingly, the server 2803 can determine that the digest for signature and the signature 3105 of the application 3104, which are transmitted from the application authentication data output means 3103 of the TRM access library section 2901 to the application authentication data input section 3106, are actually derived from the application 3104, and thus the server 2803 can authenticate the application 3104.

Fourteenth Embodiment

[0206] Fig. 33 shows the function block diagram of the application authentication system in the fourteenth embodiment of the present invention. Although the server 2803 executes a part of the authentication processing of the application downloaded to the download section 2804 in the thirteenth embodiment, application authentication is performed in a section other than the server 2803 and the server 2803 only obtains the result of authentication in this embodiment.

[0207] The terminal 2801 has the download section 2804 and the TRM access library section 2901. The download section 2804 downloads the application. The TRM access library section 2901 includes authentication success information generating means 3301 and authentication success information output means 3303.

[0208] The authentication success information generating means 3301 generates authentication success information 3302 that shows success of application authentication. In this embodiment, application authentication may be performed only in the TRM access library section 2901. Further, the TRM access library section 2901 and the authentication module 2802 may perform authentication in cooperation, and the authentication success information generating means 3301 obtains a result of the authentication to generate the authentication success information 3302 showing whether or not authentication has succeeded. At this point, the private key of the authentication module 2802 or the public key of the server 2803 may encrypt the authentication success information 3302.

[0209] The authentication success information output means 3303 outputs the authentication success information 3302 that has been generated in the authentication success information generating means 3301. If the authentication success information 3302 has not been encrypted, it may be output after the private key of the authentication module 2802 or the public key of the server 2803 encrypts the authentication success information 3302.

[0210] The authentication module 2802 has the TRM section 2805 and the TRM access library authenticating section 2902, which have the same operation as those of the thirteenth embodiment.

[0211] The server 2803 has the server TRM access library section authenticating section 2903, an authentication success information input section 3304, and a server application authenticating section 3305.

[0212] The server TRM access library section authenticating section 2903 has the same operation as that of the thirteenth embodiment.

[0213] The authentication success information input section 3304 enters the authentication success information that has been output from the authentication success information output means 3303 in the TRM access library section 2901 whose authentication has been determined as a success by the server TRM access library section authenticating section 2903. When it is determined that the TRM access library section 2901 has been successfully authenticated by the server TRM access library section authenticating section 2903, information output from the TRM access library section 2901 and the authentication module 2802 is trustworthy for the server 2803. Therefore, it can be determined that the contents of the authentication success information output means 3303 are trustworthy.

[0214] The server application authenticating section 3305 performs authentication for the application based on the authentication success information that has been input to the authentication success information input section 3304. For example, when the authentication success information output from the authentication success information output means 3303 has been encrypted by the private key of the authentication module 2802 or the public key of the server 2803, it is decrypted to check with the contents of the authentication success information and authentication is performed for the application downloaded to the download section 2804.

Fifteenth Embodiment

[0215] In the present invention, it is required to download the application and the signature in order to authenticate the application (application program). Hereinafter, description will be made for an application that stores a signature of the application therein.

[0216] The application program can be generally divided into an application main body and an application definition file. The 'application main body' is a code or data for executing the application program, and the 'ap-

plication definition file' is a file that describes an attribute of the application main body. As the 'attribute of the application main body', there exists a size of the application main body, an entry point to execute the application program, parameter (main-class starting parameter in the case of Java) that should be passed to the application program at the time of executing the application program, for example. When it is assumed that an area in which the attribute of the application main body described is referred to as an 'attribute information storage area', there are cases where an optional region that a creator of the application can freely use, exists in the attribute information storage area. Thus, signature data of the application main body may be stored in the optional region. Note that the application main body may not be the code and data itself, but may be a compression of the code and data. Similarly, the application definition file may also be a compression of an attribute description of the application main body.

[0217] Fig. 34 exemplifies an application structure of the Java application, that is, an i-application (Java application for NTT DoCoMo cell phones) in particular. In the i-application, the application main body is stored in JAR file 3401 and the application definition file is provided as an ADF file 3402. The attribute of the application main body stored in the ADF file 3402 is shown by a required key called AppName as an application name, and the size of the application main body is shown by the required key called AppSize. Furthermore, there exists an optional key shown by AppParam as the optional region that the creator of the application can freely use. A maximum of 255 bytes can be used in the region shown by the AppParam. On the other hand, 20 bytes are needed for the signature of the application main body if Elliptic Curve Cryptography of 160 bits is used, 128 bytes are needed if RSA cryptography of 1024 bits is used, and they are stored in the region shown by AppParam. Thus, the signature of the application main body can be stored in the region shown by AppParam.

[0218] Fig. 35 is the flowchart explaining a processing in performing authentication for the application that stores signature data of the application main body in the optional region in this manner. In step S3501, the signature data is obtained from the optional region. In step S3502, authentication is performed for the signature using the signature data obtained in step 3501. These steps are executable by a program.

[0219] Further, Fig. 34 can be regarded as the one showing a data structure of the application program. Specifically, it can be regarded as the one comprised of the JAR file section 3401 that stores the JAR file that is a compression file of the code and data, and the ADF file section 3402 that stores the ADF file that is the definition file of the application. In such a data structure, the ADF file of the ADF file section 3402 has a region shown by AppParam, which stores the main-class starting parameter or the like, and the signature of the JAR file stored in the JAR file section 3401 is stored in the region shown by AppParam.

[0220] The signature of the JAR file stored in the region shown by AppParam may be a signature by a person who guarantees an operation of application. Herein, the 'person who guarantees an operation of application' is a person who has created an application operated by the code and data stored in the JAR file, a person who distributes the application, a third person who verifies an operation of the application and guarantees that it does not perform an invalid operation, or the like.

[0221] Since the data structure of the application program shown in Fig. 34 can be expressed by bit stream, a recording medium such as a (SD) memory card, a flexible disc, a compact disc, or the like, on which the bit stream has been recorded, can be created.

[0222] When the application is downloaded with such an application program, not only the application main body but also the signature of the application main body is also downloaded, so that an additional task to download the signature can be omitted.

Sixteenth Embodiment

[0223] Fig. 37 exemplifies the function block diagram of the terminal according to the sixteenth embodiment of the present invention. This embodiment is characterized in that the authentication module is provided inside the terminal in the application authentication system of the first embodiment to make them unified.

[0224] In this embodiment, a terminal 3700 has a download section 3701 and a TRM section 3702.

[0225] The download section 3701 downloads the application. Specifically, it has the same function as the download section 102 in the first embodiment.

[0226] The TRM section 3702 holds the information for application authentication in the tamper-resistant region. In other words, it has the same function as the TRM section 103 in the authentication module 101 in the first embodiment.

[0227] Therefore, in the terminal of this embodiment, procedure of downloading the application or procedure of authenticating the downloaded application may be the same as the first embodiment.

[0228] By using such a terminal, in the case where the authentication processing of the application downloaded to the download section 3701 of the terminal 3700 has been performed and the authentication processing has succeeded, for example, the application can be securely permitted to access to the information stored in the terminal, such as information held by the TRM section 3702.

[0229] Although the word 'terminal' has been used, it does not mean that the word is limited to the portable terminal or the like represented by a cell phone. For example, it may be a home electronic appliance, and also may be a so-called information home electronic appliance or a network home electronic appliance. Products such as an air conditioner, a humidifier, a dehumidifier,

an air cleaner, a microwave oven, an oven, a refrigerator, a dish washing machine, a water heater, an iron, a trouser press, an electric vacuum cleaner, a washing machine, a drier, an electric blanket, electric sheets, a light fixture, a television, a radio, an audio apparatus such as a tape recorder, a camera, an IC recorder, a telephone, a facsimile machine, a copier, a printer, a scanner, a personal computer, and the like are cited. (The same will apply to the 'terminal' in the seventeenth embodiment described below.)

Seventeenth Embodiment

[0230] Fig. 38 exemplifies the function block diagram of the terminal according to the seventeenth embodiment of the present invention. This embodiment is characterized in that the authentication module is provided inside the terminal in the application authentication system of the second embodiment or the like to make the terminal and the authentication module unified.

[0231] In this embodiment, a terminal 3800 is a terminal provided with an authentication module 3801, and it has a download section 3802 and a TRM access library section 3803. The authentication module 3801 has a TRM section 3804 and a TRM access library section authenticating section 3805.

[0232] The authentication module 3801 holds information in the tamper-resistant region and performs the processing for authentication using the information. Details will be described later.

[0233] The download section 3802 downloads the application. Specifically, it has the same function as the download section 102 in the second embodiment or the like.

[0234] The TRM access library section 3803 performs the processing for application authentication on condition that the authentication module 3801 authenticates the section 3803 itself. In other words, it has the same function as the TRM access library section 401 in the second embodiment or the like. Note that 'the authentication module 3801 authenticates the section 3801 itself' means that authentication is performed by the TRM access library section authenticating section 3805, as described later.

[0235] The TRM section 3804 holds the TRM access library section authentication information in the tamper-resistant region. The TRM access library section authentication information' is information for authenticating the TRM access library section, which is the same as the definition of the second embodiment. Thus, the TRM section 3804 has the same function as the TRM section 103 of the second embodiment or the like. Note that the tamper-resistant region may be inside the TRM section 3804, or may be inside the authentication module 3801 and outside the TRM section 3804.

[0236] The TRM access library section 3805 performs authentication for the TRM access library section 3803 based on the TRM access library section authentication information. Therefore, the TRM access library section 3805 has the same function as the TRM access library section 401 of the second embodiment or the like.

[0237] Fig. 39 exemplifies the flowchart explaining the processing flow of the terminal 3800 in this embodiment. It is presumed that the application has been downloaded to the download section 3802 in the processing exemplified in this flowchart.

[0238] In step S3901, the TRM access library section authenticating section 3805 performs authentication processing of the TRM access library section 3803.

[0239] In step S3902, whether or not the TRM access library section 3803 has been authenticated is determined, and the processing proceeds to step S3903 if authenticated. In Fig. 39, the processing ends if it has not been authenticated. Instead, the application downloaded to the download section 3802 may be discarded.

[0240] In step S3903, the TRM access library section 3803 performs authentication processing of the application downloaded to the download section 3802.

[0241] In step S3904, if the downloaded application has been authenticated, the processing proceeds to step S3905. If it has not been authenticated, the processing ends. Instead of ending the processing, the application downloaded to the download section 3802 may be discarded.

[0242] In step S3905, access of the downloaded application to the authentication module is permitted. It is the authentication module 3801 that permits the access. Alternatively, if the function of the TRM access library section 3803 is always used when the application accesses the authentication module 3803, access by the TRM access library section 3803 to the authentication module may be permitted.

[0243] Note that the TRM access library section 3803 may comprise the application manager, the device driver, or the like as described in the second embodiment.

[0244] According to this embodiment, when the terminal has the authentication module inside thereof, the terminal can hold information that must be highly protected inside thereof, and authentication for the application downloaded to the terminal can be performed. Eighteenth Embodiment

[0245] The eighteenth embodiment of the present invention relates to the application authentication system that comprises a primary equipment and an authentication module. In this embodiment, authentication for the application stored in the primary equipment is performed by using information held in the authentication module.

[0246] Fig. 40 exemplifies the function block diagram of the application authentication system of this embodiment. The application authentication system comprises a primary equipment 4001 and an authentication module 4002. The primary equipment is not limited to the terminal, but may be a personal computer, a workstation, a large-scale computer, or a server. Further, the primary equipment 4001 and the authentication module

4002 do not need to be directly connected electrically, nor do they need to be contacted physically. For example, they may be connected via radio waves. Alternatively, they may be connected via a network represented by the Internet. Particularly, the network may be constructed using a medium such as an optical cable that does not use electrical transmission.

[0247] The primary equipment 4001 comprises an application storage section 4003. The application storage section 4003 stores the application. The application is not limited to a program that operates in the primary equipment 4001. It may be the application that operates in equipment other than the primary equipment 4001. Further, to 'store' is to hold the application. The length of holding time is unlimited. An object of holding the application is unlimited as well. For example, the object of storage may be that the application is made to operate in the primary equipment 4001. Further, the object may be that the application is downloaded to the primary equipment 4001 and made to operate. Alternatively, the object may be a temporary holding for the primary equipment 4001 to relay the application when it is sent via a communication network. Alternatively, the object may be that the application is held to download it to equipment other than the primary equipment 4001.

[0248] The authentication module 4002 comprises a TRM section 4004. The TRM section 4004 holds information for an authentication processing of the application in the tamper-resistant region. As the information for processing application authentication, the private key for encryption, a certificate to confirm authenticity of the signature of the application, or the like, is cited for example. The application referred to here is an application stored in the application storage section 4003 of the primary equipment 4001. Accordingly, the TRM section of the authentication module in this embodiment may be the one having the same function as the TRM section of the first embodiment. In this case, a method of processing application authentication, or the like is the same as that of the embodiment.

[0249] Since authentication can be performed for the application stored in the application storage section 4003 with the application authentication system of this embodiment, the application is prevented from operating obliquely, for example.

[0250] Note that the primary equipment 4001 may be a home electronic appliance. It also may be a so-called information home electronic appliance or a network home electronic appliance. Products such as an air conditioner, a humidifier, a dehumidifier, an air cleaner, a microwave oven, an oven, a refrigerator, a dish washing machine, a water heater, an iron, a trouser press, an electric vacuum cleaner, a washing machine, a drier, an electric blanket, electric sheets, a light fixture, a television, a radio, an audio apparatus such as a tape recorder, a camera, an IC recorder, a telephone, a facsimile machine, a copier, a printer, a scanner, a personal computer, and the like are cited.

Nineteenth Embodiment

[0251] The nineteenth embodiment of the present invention also relates to the application authentication system that comprises a primary equipment and an authentication module similar to the eighteenth embodiment. In this embodiment, when authentication is performed for the application stored in the primary equipment, the authentication module authenticates a section in the first equipment, which performs authentication.

[0252] Fig. 41 exemplifies the function block diagram of the application authentication system in this embodiment. The application authentication system comprises a primary equipment 4101 and an authentication module 4102. Note that the primary equipment 4101 and the authentication module 4102 do not need to be directly connected electrically, nor do they need to be connected physically, as in the eighteenth embodiment.

[0253] The primary equipment 4101 comprises an application storage section 4103 and a TRM access library section 4104.

[0254] The application storage section 4103 stores the application. For example, it has the same function as the application storage section 4003 in the eighteenth embodiment.

[0255] The TRM access library section 4104 performs the processing for application authentication on condition that the authentication module 4102 authenticates the section 4104 itself. Herein, the 'itself' means the TRM access library section 4104. Alternatively, the 'itself' may be a section that includes the TRM access library section 4104. For example, the primary equipment 4101 may be the 'itself'.

[0256] Further, the 'application' means the application stored in the application storage section 4003.

[0257] Therefore, the processing in which the authentication module authenticates the TRM access library section 4104 itself is performed, and the processing for authenticating the application stored in the application storage section 4103 is performed when it has been correctly authenticated as a result of the processing.

[0258] Note that the TRM access library section 4104 may comprise the application manger and the device driver and performs their processing, as described in the second embodiment.

[0259] The authentication module 4102 comprises the TRM section 4105 and a TRM access library section authenticating section 4106.

[0260] The TRM section 4105 holds the TRM access library section authentication information in the tamper-resistant region. The 'TRM access library section authentication information' is information for authenticating the TRM access library section. For example, information for specifying the primary equipment is cited. Such information as: a manufacturer name and a production number, and a telephone number if the telephone number is allocated for the primary equipment. Further, the information may be the one showing a state

where the primary equipment is placed, such as information of another equipment to which the primary equipment is connected, information that specifies a part equipped to the primary equipment, or a version number of a program installed in the primary equipment. Furthermore, when the primary equipment is capable of holding secret information of any kind such as an encryption key, information for detecting that the encryption key is authentic may be the TRM access library section authentication information.

[0261] In addition, refer to the description of the second embodiment for the tamper-resistant region.

[0262] The TRM access library section authenticating section 4106 performs authentication for the TRM access library section 4104 of the primary equipment 4101 based on the TRM access library section authentication information. Specifically, it obtains the information sent from the TRM access library section 4104, determines whether or not the information obtained from the TRM access library section 4104 conforms to the TRM access library section authentication information, and performs authentication processing.

[0263] Note that an object for which the TRM access library section authenticating section 4106 performs authentication is not limited to the TRM access library section 4104, but may be a section including the TRM access library section 4104. For example, the section 4106 may perform authentication for the entire primary equipment 4101. In this case, the TRM access library section authentication information may use the production number of the first equipment 4101 or the state where the primary equipment 4101 is placed.

[0264] Fig. 42 exemplifies the flowchart that explains the operation of the application authentication system in this embodiment.

[0265] In step S4201, the TRM access library section authenticating section 4106 performs authentication processing of the TRM access library section 4104. At this point, the TRM access library section authentication information held in the tamper-resistant region is used.

[0266] In step S4202, it is determined that whether or not the TRM access library section 4104 has been authenticated by the processing of step S4201. If it has been determined that the section 4104 was authenticated, the TRM access library section 4104 performs authentication processing of the application stored in the application storage section 4103, in step S4203.

[0267] In this embodiment, the TRM access library section 4104, which has been authenticated by the TRM access library section authenticating section 4106 of the authentication module 4102, performs application authentication. Thus, the result of application authentication is trustworthy for the authentication module 4102. As a result, in the case where access to the authentication module has occurred by execution of the application stored in the application storage section 4103, the authentication module can permit the access. Further, even if the application storage section 4103 has been provided to download the application to another equipment, for example, access from the application downloaded from the application storage section 4103 to the authentication module can be permitted. Furthermore, information showing that the application has been authenticated by the authentication module 4102 can be added to the application. This can realize a processing more complicate than the conventional processing.

Twentieth Embodiment

[0268] The application authentication system shown in the nineteenth embodiment or the like has been constituted of 2 kinds of principal equipment of the primary equipment and the authentication module. However, the number of the principal equipment is not limited to 2 as shown in this embodiment.

[0269] Fig. 43 exemplifies the function block diagram of the application authentication system when the number of principal equipment is 3. The application authentication system comprises a first equipment 4301, a second equipment 4302, and a third equipment 4303. Specifically, the application authentication system has 3 principal sections. Note that the 3 principal sections are connected in series, but they do not need to be directly connected electrically nor do they need to be contacted physically, as described in the eighteenth embodiment and the nineteenth embodiment. Further, a person who owns or occupies the first equipment 4301, the second equipment 4302, and the third equipment 4303 may be one, or the 3 kinds of equipment may be owned or occupied by different persons.

[0270] Correspondence with the application authentication system of the nineteenth embodiment or the like is as follows. In other words, the first equipment 4301 is equivalent to the authentication module, and the third equipment 4303 is equivalent to the terminal or the primary equipment 4101 in the nineteenth embodiment.

[0271] The first equipment 4301 comprises a TRM section 4304 and a first authentication processing section 4305.

[0272] The TRM section 4304 holds the authentication information for authenticating the second equipment 4302 in the tamper-resistant region. Therefore, it has the same function as the TRM section in the nineteenth embodiment. But, what is different is that the information held in the tamper-resistant region is the authentication information for authenticating the second equipment. Note that the tamper-resistant region does not only hold the information to authenticate the second equipment but may also hold the information to authenticate the third equipment. As the authentication information, the information showing the production number of the equipment or the state where the equipment is placed, or the information for detecting the authenticity of an encryption key or a certificate if the equipment can hold the encryption key or the certificate is cited, similar to the TRM access library section authentication infor-

mation in the nineteenth embodiment.

[0273] The first authentication processing section 4305 performs authentication for the second equipment 4302 based on the authentication information. The 'authentication information' is the authentication information held in the tamper-resistant region.

[0274] The second equipment 4302 comprises a second authentication processing section 4306. The second authentication processing section 4306 performs authentication for the third equipment 4303 on condition that the first authentication processing section 4305 authenticates the equipment 3402 itself. Herein, the 'itself' means the second equipment 3402 including the second authentication processing section 4306.

[0275] In the case where the first authentication processing section 4305 has authenticated the second equipment 4302, the second equipment 4302 can be regarded as trustworthy equipment for the first equipment 4301. Therefore, the first equipment 4301 can permit the second equipment 4302 to access to the information held in the tamper-resistant region. Then, when the second authentication processing section 4306 performs authentication for the third equipment 4303, it can use the information held in the tamper-resistant region. Accordingly, the second authentication processing section 4306 may use the information held in the tamper-resistant region when it performs authentication for the third equipment 4303.

[0276] As described, the second authentication processing section 4306 may include a function of the device driver for accessing to the first equipment 4301.

[0277] Further, the second authentication processing section 4306 may obtain information necessary to perform authentication for the third equipment 4303 from equipment different from the first equipment or the third equipment. In obtaining the information, the second authentication processing section 4306 may present information showing that the second equipment 4302 has been authenticated by the first authentication processing section 4305.

[0278] The third equipment 4303 comprises an application storage section 4307 and a third authentication processing section 4308. The application storage section 4307 stores the application. Therefore, it has the same function as the application storage section in the nineteenth embodiment or the like. Thus, the length of time to store the application or an object of storage is not particularly limited.

[0279] The third authentication processing section 4308 performs the processing for authenticating the application on condition that the second equipment 4302 authenticates the equipment 4303 itself. The 'application' means the application stored in the application storage section 4307. Further, the 'itself' means the third equipment 4303.

[0280] In the case where the second authentication processing section 4306 has authenticated the third equipment 4303, the third equipment 4303 can be regarded as trustworthy equipment for the first equipment 4301. Therefore, the first equipment 4301 can permit the third equipment 4303 to access to the information held in the tamper-resistant region. Then, when the third authentication processing section 4308 performs authentication for the application, it can use the information held in the tamper-resistant region.

[0281] Further, the third authentication processing section 4308 may obtain information necessary to perform authentication for the application from equipment different from the first equipment or the second equipment. In obtaining the information, the third authentication processing section 4308 may present information showing that the third equipment 4303 has been authenticated by the second authentication processing section 4306. Alternatively, in such an occasion, the second equipment 4302 may present information that the second equipment 4302 has been authenticated by the first authentication processing section 4305.

[0282] Fig. 44 exemplifies the flowchart that explains the operation of the first equipment 4301. In step 4401, the first authentication processing section 4305 obtains the authentication information that the TRM section 4304 holds in the tamper-resistant region. In step S4402, authentication processing of the second equipment is performed, and whether or not it has been authenticated is determined in step S4403. If the equipment has been authenticated, the fact that it has been authenticated is transmitted to the second equipment in step S4404.

[0283] Fig. 45 exemplifies the flowchart that explains the operation of the second equipment 4302. In step S4501, whether or not it has been authenticated by the first authentication processing section 4305 is determined. This determination is made depending on whether or not the fact that the first equipment 4301 was authenticated in step S4404 shown in Fig. 44 has been transmitted from the first equipment. If it has been authenticated, the second authentication processing section 4306 performs authentication processing of the third equipment, in step S4502. In step S4503, whether or not it has been authenticated is determined. If the equipment has been authenticated, the fact that it has been authenticated is transmitted to the third equipment in step S4504.

[0284] Fig. 46 exemplifies the flowchart that explains the operation of the third equipment 4303. In step S4601, whether or not it has been authenticated by the second authentication processing section 4306 is determined. This determination is made depending on whether or not the fact that the second equipment 4302 was authenticated in step S4504 shown in Fig. 45 has been transmitted from the second equipment. If it has been authenticated, authentication processing of the application is performed in step S4602. Although the processing ends here in Fig. 46, the result of processing for application authentication may be transmitted to the first equipment 4301, for example. Alternatively, it may be

transmitted to the second equipment 4302. Furthermore, if the application accesses another piece of equipment, it may present information showing that it has been authenticated by the third authentication processing section 4308. Alternatively, the application may be added with information showing that it has been authenticated by the third authentication processing section 4308.

[0285] The case described above has been the one in which the application authentication system is constituted of 3 kinds of principal equipment, but the application authentication system may be constituted of 4 kinds of principal equipment as shown in Fig. 47.

[0286] In Fig. 47, the application authentication system comprises a first equipment 4701, a second equipment 4702, a third equipment 4703, and a fourth equipment 4704. The first equipment 4701 comprises a TRM section 4705 and a first authentication processing section 4706, which correspond to the TRM section 4304 and the first authentication processing section 4305 exemplified in Fig. 43. The second equipment 4702 comprises a second authentication processing section 4707. This corresponds to the second authentication processing section 4306 exemplified in Fig. 43.

[0287] The third equipment has a third authentication processing section 4708. The third authentication processing section 4708 performs authentication for the fourth equipment 4704 on condition that the section 4708 itself is authenticated by the second authentication processing section 4707. If the second authentication processing section 4707 authenticates the third equipment 4703, the third equipment 4703 becomes trustworthy equipment for the first equipment 4701. Therefore, the first equipment 4701 can permit the third equipment 4703 to access to the information that the TRM section 4705 holds in the tamper-resistant region. Then, the third authentication processing section 4708 obtains the information that the TRM section 4705 holds in the tamper-resistant region, and may perform authentication for the fourth equipment 4704. Alternatively, it may obtain the information held in another equipment to perform authentication.

[0288] In the case where the third authentication processing section 4708 obtains the information that the TRM section 4705 holds in the tamper-resistant region, a communication section may be provided for the third equipment 4703 and the first equipment 4701 to enable the third equipment 4703 and the first equipment 4701 to directly communicate with each other. Alternatively, the following can be performed when the second authentication processing section 4707 includes the device driver function to access to the first equipment 4701. Specifically, the third authentication processing section 4708, by using the device driver function provided by the second authentication processing section 4707, obtains the information that the TRM section 4705 has in the tamper-resistant region via the second equipment. Therefore, the third authentication processing section 4708 may include the device driver function to access to the second authentication processing section 4707.

[0289] The fourth equipment 4704 has an application storage section 4709 and a fourth authentication processing section 4710. The application storage section 4709 corresponds to the application storage section 4307 in Fig. 43. The fourth authentication processing section 4710 performs authentication on condition that the equipment 4704 itself is authenticated by the third authentication processing section 4708. Herein the 'itself' means the fourth equipment 4704. Accordingly, if the third authentication processing section 4708 has authenticated the fourth equipment 4704, it is regarded that the first authentication processing section 4706 has authenticated the equipment, so that the third authentication processing section 4710 can perform authentication for the application stored in the application storage section 4709 using the information that the TRM section 4705 holds in the tamper-resistant region. Further, the fourth authentication processing section 4710 presents information showing that it has been authenticated the third authentication processing section 4708 for another equipment, obtains information for application authentication, and may perform authentication for the application.

[0290] Thus, an operation in the case where the application authentication system is constituted of the 4 kinds of principal equipment is as follows. The operation of the first equipment 4701 is the same as the one exemplified in Fig. 44. Similarly, the operation of the second equipment 4702 is exemplified in Fig. 45. The operation of the third equipment 4703 is exemplified in Fig. 48. In other words, whether or not the third equipment 4703 has been authenticated by the second authentication processing section 4707 is determined in step S4801. If it has been authenticated, the authentication processing of the fourth equipment 4704 is performed in step S4802. In step S4803, whether or not it has been authenticated is determined, and if authenticated, the fact that it has been authenticated is transmitted to the fourth equipment 4704 in step S4804.

[0291] The operation of the fourth equipment 4704 is exemplified in Fig. 49. Whether or not it has been authenticated by the third authentication processing section 4708 is determined in step S4901, and if authenticated, the authentication processing of the application is performed in step 4902. The result of the authentication processing of the application may be transmitted to the first equipment 4701, for example. Alternatively, it may be transmitted to the second equipment 4702. If the application accesses another equipment, the information showing it has been authenticated by the third authentication processing section 4708 may be presented. Alternatively, the application may be added with the information showing that it has been authenticated by the third authentication processing section 4708.

[0292] Moreover, the number of principal equipment

is not limited to 4, but the application authentication system may be constituted of 5 kinds of equipment as shown in Fig. 50, which are a first equipment 5001, a second equipment 5002, a third equipment 5003, a fourth equipment 5004, and a fifth equipment.

[0293] Fig. 51 exemplifies the function block diagram of the application authentication system when the number of principal equipment is generalized. In Fig. 51, the application authentication system is constituted of (N+1) pieces of equipment, which is formed by connecting a first equipment 5101 through an (N+1)th equipment 5105 in series. The description 'connecting' does not only mean that they are directly connected electrically or physically contact with each other. For example, they may be connected by a network represented by the Internet. Particularly, they may be connected by the network using the optical cable. Further, they may be connected by radio waves. In addition, the equipment may be interconnected with each other.

[0294] The first equipment 5101 has a TRM section 5106 and a first authentication processing section 5107. The TRM section 5106 holds information for authenticating the second equipment 5102 in the tamper-resistant region. The first authentication processing section 5107 performs authentication for the second equipment 5102 based on the authentication information.

[0295] In the following, any one of the second equipment 5102 to the N-th equipment 5104 will be shown as an i-th equipment. The i-th equipment has an i-th authentication processing section. The i-th authentication processing section performs authentication for an (i+1) th equipment on condition that the equipment itself is authenticated by the i-th authentication processing section. Herein, the 'itself' means the i-th equipment. Therefore, the i-th authentication processing section performs authentication for the (i+1)th equipment if the i-th equipment has been authenticated by an (i-1)th authentication processing section. If the (i-1)th authentication processing section has authenticated the i-th equipment, the i-th equipment can be regarded as a trustworthy one for the first equipment 5101. Thus, the first equipment 5101 can permit the i-th equipment to access to the information held in the tamper-resistant region by the TRM section 5106. Then, the i-the equipment may perform authentication for the (i+1)th equipment using the information held in the tamper-resistant region.

[0296] For example, in the case where the i-th authentication processing section accesses to the information held in the tamper-resistant region by the TRM section 5106, the i-th equipment and the first equipment 5101 may directly communicate with each other.

[0297] Further, the i-th authentication processing section may include the device driver function or the like to access to the (i-1)th authentication processing section. With this function included, an information demand is sequentially output from the i-th authentication processing section to the first authentication processing section 5107, and the demanded information is sent back sequentially from the first authentication processing section 5107 to the i-th authentication processing section.

[0298] The (N+1)th equipment has an application storage section 5111 and an (N+1)th authentication processing section 5112. The application storage section 5111 stores the application. Time for storing the application is unlimited. For example, the application may be stored to execute the application in the (N+1)th equipment 5105, or may be temporarily stored only to relay application transmission. Furthermore, an object of application storage is no object, and it is not only stored to execute the application in the (N+1)th equipment 5105, but may be stored for a downloading purpose to execute the application in another equipment. In addition, it may be stored to download and execute the application in the (N+1)th equipment 5105. Note that the name 'application' has been used, but it is not necessarily a program, but may be data.

[0299] The (N+1) th authentication processing section 5112 performs authentication for the application on condition that the equipment itself is authenticated by an N-th authentication processing section 5110. The 'itself' means the (N+1)th equipment 5105, and the 'application' means the application stored in the application storage section 5111.

[0300] Fig. 52 is the flowchart explaining the operation of any equipment from the second equipment 5102 to the N-th equipment 5104. In step S5201, whether or not the equipment has been authenticated by the (i-1)th authentication processing section is determined, and if authenticated, the authentication processing of the (i+1)th equipment is performed in step S5202. Whether or not the (i+1)th equipment has been authenticated is determined in step S5203, and if authenticated, the fact that the it has been authenticated is transmitted to the (i+1) th equipment. Thus, authentication is performed from the second equipment 5102 to the N-th equipment 5104 sequentially.

[0301] Fig. 53 exemplifies the flowchart of the operation of the (N+1)th equipment 5105. Whether or not it has been authenticated by the N-th authentication processing section 5110 is determined in step S5301, and if it is determined that it has been authenticated, it performs the authentication processing of the application in step S5302. When the application has been authenticated, the equipment 5105 transmits its result to the first equipment 5101 or the like, and permits the application to access to the first equipment 5101. Alternatively, the information that the application has been authenticated may be added to the application.

[0302] In Figs. 43, 47, 50, and 51, the equipment has been connected in series, but the equipment may be connected by using the nested structure. Fig. 54 schematically shows that the equipment is connected using the nested structure. A secure device 5401 is equivalent to the first equipment 5101, and has the TRM section and the first authentication processing section. The secure device 5401 is connected so as to be built in an

adapter 5402 that is equivalent to the second equipment, as a part thereof. The adapter 5402 is connected so as to be built in a communication module 5403 that is equivalent to the third equipment, as a part thereof. Further, the communication module 5403 is connected so as to be built in a PDA (personal digital assistance) 5404 that is equivalent to the fourth equipment, as a part thereof. The PDA 5404 is connected to the server, which is equivalent to the fifth equipment, via a communication line. With such a connection, authentication can be performed for the application stored in the server 5405 by using the information held in the tamper-resistant region of the secure device 5401.

[0303] Note that the (N+1)th equipment 5105 may be a home electronic appliance. It also may be a so-called information home electronic appliance or a network home electronic appliance. Products such as an air conditioner, a humidifier, a dehumidifier, an air cleaner, a microwave oven, an oven, a refrigerator, a dish washing machine, a water heater, an iron, a trouser press, an electric vacuum cleaner, a washing machine, a drier, an electric blanket, electric sheets, a light fixture, a television, a radio, an audio apparatus such as a tape recorder, a camera, an IC recorder, a telephone, a facsimile machine, a copier, a printer, a scanner, a personal computer, and the like are cited.

Twenty-first Embodiment

[0304] In the twenty-first embodiment, when any one of the second equipment to the N-th equipment is shown as the i-th equipment, the i-th equipment may hold the information necessary for authenticating the (i+1)th equipment. For example, the i-th equipment has the tamper-resistant region, and may hold the necessary information for performing authentication in the region.

[0305] As described, when there could be a case that the i-th equipment holds the authentication information, which is the information necessary for authenticating, the i-th equipment may have an i-th authentication information obtaining section. Herein, the i-th authentication information obtaining section is a section that obtains the authentication information from an authentication information storage region when the i-th equipment has the authentication information storage region that is a region storing the authentication information. Further, the i-th authentication information obtaining section obtains the authentication information from the TRM section via the equipment from the second equipment to the (i-1)th equipment when the TRM section of the first equipment stores the authentication information. 'Via the equipment from the second equipment to the (i-1)th equipment' means the following. Specifically, the i-th authentication information obtaining section outputs a demand of the authentication information to an (i-1)th authentication information obtaining section, and finally, a second authentication information obtaining section outputs a demand of the authentication information to the first equipment. When the second authentication information obtaining section obtains the authentication information from the first equipment, it outputs the authentication information to a third authentication information obtaining section, and finally, the (i-1)th authentication information obtaining section outputs the authentication information to the i-th authentication information obtaining section.

[0306] Fig. 55 exemplifies the flowchart explaining the operation of the i-th equipment in this embodiment. In step S5501, whether or not it has been authenticated by the (i-1)th authentication processing section is determined. When it is determined that it has been authenticated, the processing proceeds to step S5502, and whether or not the authentication information of the (i+1)th equipment is stored in the authentication information storage region is determined. For example, the i-th equipment reads out the information stored in the authentication information storage region and determines if the authentication information can be obtained. If the information has not been stored, the processing proceeds to step S5503, and the equipment obtains the authentication information from the TRM section via the second equipment to the (i-1)th equipment. In step S5504, the authentication processing of the (i+1)th equipment is performed, and whether or not it has been authenticated is determined in step S5605. If authenticated, the fact that it has been authenticated is transmitted to the (i+1)th equipment.

[0307] By performing such a processing, even if the number of equipment that constitutes the application authentication system increases, authentication is performed using the authentication information when the equipment has the authentication information, and for example, it is possible to complete authentication for all the equipment in a short time.

Advantage of the Invention

[0308] As described above, according to the present invention, the authentication module and the terminal are combined to authenticate the application that operates in the terminal by the information held in the authentication module, and thus preventing an undesirable application from being executed in the terminal.

[0309] Further, by authenticating the TRM access library in the terminal with the authentication module, the TRM access library can perform a processing for authenticating the application. As a result, an application with high security can be executed, and an operation of A business transaction using the terminal can be performed. In addition, the tamper-resistant region may be in the authentication module and there is no need to mount the tamper-resistant region on the terminal, thus reducing manufacturing costs.

[0310] Furthermore, a source of the application is guaranteed by authenticating the application that operates in the terminal, and the application is permitted to

access to the local resources of the terminal or the authentication module.

[0311] Still further, by authenticating the TRM section of the authentication module with the server, authentication for the terminal and the application that operates in the terminal can be performed. Thus; highly confidential information can be exchanged with the application that operates in the terminal, and an operation of complicated business transaction can be realized among the server, the terminal, and the authentication module.

[0312] Still further, by storing the signature of the application main body in the optional region, the signature of the application main body can be simultaneously downloaded with download of the application, thus the additional task to download the signature of the application main body can be omitted.

[0313] Moreover, in a state where three or more kinds of equipment are connected in series, authentication is sequentially performed from the equipment on one end and authentication for the application stored in the equipment on the other end.

Claims

1. An application authentication system that comprises a terminal and an authentication module, wherein

   the terminal includes a download section to download an application, and

   the authentication module includes a TRM section that holds information for a processing of application authentication in a tamper-resistant region.

2. An application authentication system that comprises a terminal and an authentication module, wherein

   the terminal includes a download section to download an application; and

   a TRM access library section that performs a processing for application authentication on condition that the TRM access library section itself is authenticated by the authentication module, and

   the authentication module includes: a TRM section that holds TRM access library section authentication information, which is information to perform authentication for the TRM access library, in a tamper-resistant region; and

   a TRM access library section authenticating section that performs authentication for the TRM access library section of the terminal based on the TRM access library section authentication information.

3. The application authentication system according to Claim 2, wherein

   the download section of the terminal downloads an application added with a signature, which is information used to authenticate that the application has not been tampered with,

   the TRM access library section generates digest for signature authentication from the application downloaded to the download section,

   the terminal further includes a signature authentication information output section that outputs signature authentication information including the digest for signature authentication, which has been generated, and the signature to the authentication module, and

   the authentication module further includes: a signature authentication information input section that enters the signature authentication information output from the signature authentication information output section; and

   a signature authentication section that performs verification for the signature based on the digest for signature authentication and the signature, which are entered from the signature authentication information input section.

4. The application authentication system according to Claim 3, wherein

   the authentication module further includes a signature-derived digest generation information obtaining section that obtains signature-derived digest generation information to generate a signature-derived digest by using the signature entered from the signature authentication information input section; and

   a signature-derived digest generation section that generates the signature-derived digest by using the signature entered from the signature authentication information input section and the signature-derived digest generation information held in the signature-derived digest generation information obtaining section, and

   the signature authentication section performs authentication based on the signature-derived digest that has been generated in the signature-derived digest generation section and the digest for signature authentication, which has been entered from the signature authentication information input section.

5. The application authentication system according to any one of Claims 2 to 4, wherein

   the terminal includes an authentication module authenticating section for authenticating the authentication module.

6. The application authentication system according to Claim 5, wherein

   the TRM access library section includes application-usable resource information holding means that holds application-usable resource infor-

mation that is information regarding resources whose use is approved for an authenticated application.

7. The application authentication system according to any one of Claims 5 and 6, wherein

the TRM access library section of the terminal further includes application-usable resource information output means that outputs the application-usable resource information to the TRM section of the authentication module for which authentication by the authentication module authenticating section has been performed, and

the TRM section of the authentication module holds the application-usable resource information, which has been output from the application-usable resource information output means, in a tamper-resistant region in a rewritable manner.

8. The application authentication system according to any one of Claims 6 and 7, wherein

the TRM access library section approves use of resources for an application based on the application-usable resource information.

9. The application authentication system according to any one of Claims 6 to 8, wherein

the terminal includes an application-usable resource information download section that downloads application-usable resource information added with a signature, and

the TRM access library section verifies the signature added to the application-usable resource information that has been downloaded to the application-usable resource information download section.

10. The application authentication system according to any one of Claims 6 to 8, wherein

the terminal includes an application-usable resource information download section that downloads application-usable resource information added with a signature,

the TRM access library section generates a digest for signature authentication from the application-usable resource information that has been downloaded to the application-usable resource information download section,

the terminal further includes a signature authentication information output section for application-usable resource information, which outputs signature authentication information including the digest for signature authentication, which has been generated, and the signature to the authentication module, and

the authentication module further includes: a signature authentication information input section for application-usable resource information, which enters the signature authentication information output from the signature authentication information input section for application-usable resource information; and

a signature authentication section for application-usable resource information, which performs verification for the signature based on the digest for signature authentication and the signature, which are entered from the signature authentication information input section for application-usable resource information.

11. The application authentication system according to Claim 2, wherein

the TRM access library section authentication information is information unique to the terminal.

12. The application authentication system according to Claim 2, wherein

the TRM access library section authentication information is information regarding a combination of applications installed'to the terminal.

13. The application authentication system according to Claim 2, wherein

the TRM access library section authentication information is library identification information that is information for identifying the TRM access library section.

14. The application authentication system according to any one of Claims 2 to 4, wherein

the terminal includes a terminal application holding section that holds a terminal application that accesses to the TRM section of the authentication module,

the TRM section of the authentication module includes an in-authentication-module application holding section that holds an in-authentication-module application, which operates in the authentication module, in the tamper-resistant region, and

the in-authentication-module application accepts access from the terminal application and operates on condition that the TRM access library section authenticating section succeeds in authenticating the TRM access library section.

15. The application authentication system according to Claim 14, wherein

the TRM section of the authentication module includes authentication result identifier generating means that generates an authentication result identifier on condition that the TRM access library section authenticating section succeeds in authenticating the TRM access library section, and

an in-authentication-module application enables the terminal application to access to the in-authentication-module application on condition that

the authentication result identifier showing authentication success exists, and the in-authentication-module application accepts access from the terminal application.

16. The application authentication system according to Claim 14, wherein

the TRM section of the authentication module includes application authentication result identifier generating means that generates an application authentication result identifier on condition that the TRM access library section succeeds in authenticating the application, and

an in-authentication-module application enables the terminal application to access the in-authentication-module application on condition that the application authentication result identifier showing authentication success exists, and the in-authentication-module application accepts access from the terminal application.

17. An application authentication system that comprises a terminal, an authentication module, and a server that downloads an application to the terminal, wherein

the terminal includes a download section to download the application,

the authentication module includes a TRM section that holds information for a processing of application authentication in a tamper-resistant region, and

the server includes a terminal authentication section, which determines that authentication for the terminal has succeeded on condition that authentication for the authentication module via the terminal succeeds.

18. An application authentication system that comprises a terminal, an authentication module, and a server that downloads an application to the terminal, wherein

the terminal includes: a download section to download the application; and

a TRM access library section that performs a processing for application authentication on condition that the TRM access library section itself is authenticated by the authentication module,

the authentication module includes: a TRM section that holds TRM access library section authentication information, which is information for authenticating the TRM access library section, in a tamper-resistant region; and

a TRM access library section authenticating section that performs authentication for the TRM access library section of the terminal based on the TRM access library section authentication information, and

the server includes a server TRM access library section authenticating section, which determines that authentication for the TRM access library section has succeeded on condition that authentication for the TRM section of the authentication module succeeds via the TRM access library section of the terminal.

19. An application authentication system that comprises a terminal, an authentication module, and a server that downloads an application to the terminal, wherein

the terminal includes: a download section to download the application;

digest for signature generating means that generates a digest for signature from the application;

downloaded application signature obtaining means that obtains a signature downloaded along with the application; and

a TRM access library section that has application authentication data output means that transmits the obtained signature and the digest for signature generated by the digest for signature generating means,

the authentication module includes: a TRM section that holds TRM access library section authentication information, which is information for authenticating the TRM access library section, in a tamper-resistant region; and

a TRM access library section authenticating section that performs authentication for the TRM access library section based on the TRM access library section authentication information, and

the server includes: a server TRM access library section authenticating section, which determines that authentication for the TRM access library section has succeeded on condition that authentication for the TRM section of the authentication module succeeds via the TRM access library section of the terminal;

an application authentication data input section that enters the digest for signature and the signature, which have been output from application authentication data output means of the TRM access library section whose authentication by the server TRM access library section authenticating section is determined to have succeeded; and

a server application authenticating section that performs authentication for the application based on the digest for signature and the signature input to the application authentication input section.

20. An application authentication system that comprises a terminal, an authentication module, and a server that downloads an application to the terminal, wherein

the terminal includes: a download section to download the application; and

a TRM access library section having:

authentication success information generating means that generates authentication success information showing success of application authentication; and
application authentication success information output means that outputs the authentication success information generated in the authentication success information generating means,
the authentication module includes: a TRM section that holds TRM access library section authentication information, which is information for authenticating the TRM access library section, in a tamper-resistant region; and
a TRM access library section authenticating section that performs authentication for the TRM access library section based on the TRM access library section authentication information, and
the server includes: a server TRM access library section authenticating section, which determines that authentication for the TRM access library section has succeeded on condition that authentication for the TRM section of the authentication module succeeds via the TRM access library section of the terminal;
an authentication success information input section that enters the authentication success information that has been output from the authentication success information output means of the TRM access library section, whose authentication by the server TRM access library section authenticating section is determined to have succeeded; and
a server application authenticating section that performs authentication for the application based on the authentication success information input to the authentication success information input section.

21. An application program that comprises an application main body and an application definition file, wherein
the application definition file includes an optional region that a creator of the application can freely use in an attribute information storage area, which is an area to store information showing the attribute of the application main body, and stores signature data of the application main body in the optional region, said application program causing a computer to execute procedures for:

obtaining the signature data from the optional region; and
verifying the signature using the signature data obtained.

22. The application program according to Claim 21, wherein
the application program is an i-application, and the optional region is AppParam.

23. A data structure of an application program, comprising:

a JAR file section that stores a JAR file, which is a compression file of code and data; and
an ADF file section that stores an ADF file, which is a definition file of an application, wherein
the ADF file has AppParam that stores main-class starting parameter, and
a signature of the JAR file is stored in the AppParam.

24. The data structure according to Claim 23, wherein
the signature of the JAR file is a signature of a person who guarantees an operation of the application program.

25. A storage medium in which an application program is stored in a computer-readable manner by the data structure according to any one of Claims 23 and 24.

26. The application authentication system according to Claims 2 to 4, wherein
the download section downloads a use license added with a signature, which describes application-usable resource information of a downloaded application.

27. The application authentication system according to Claim 26, wherein
said application-usable resource information is a type of local resource.

28. The application authentication system according to Claim 26, wherein
said application-usable resource information is a range in which use of local resources is approved.

29. The application authentication system according to Claim 18, wherein
the TRM access library section performs a processing for application authentication on condition that the application has accessed the tamper-resistant region of the TRM section of the authentication module.

30. The application authentication system according to Claim 18, wherein
the TRM access library section performs a processing for application authentication on condi-

tion that the application has been downloaded to the download section.

31. The application authentication system according to Claim 18, wherein
the TRM access library section performs a processing for application authentication by using a start of application execution as a trigger.

32. The application authentication system according to Claim 26, wherein
the application-usable resource information of the use license includes expiry date information showing a time limit for accessing to resources, and
the download section downloads the use license when the time limit approved based on said expiry date information has already expired.

33. The application authentication system according to Claims 2 to 4, wherein
the download section downloads a use license from a server at the time of executing the application that has been downloaded or/and at the time of performing authentication for the application.

34. The application authentication system according to Claim 26, wherein
the download section inquires a server of validity of the downloaded use license at the time of executing the application that has been downloaded or/and at the time of performing authentication for the application.

35. A terminal according to any one of Claims 1 to 21, and 26 to 34.

36. An authentication module according to any one of Claims 1 to 21.

37. A terminal, comprising:

a download section that downloads an application; and
a TRM section that holds information for a processing of application authentication in a tamper-resistant region.

38. A terminal that includes an authentication module to hold information in a tamper-resistant region and to perform a processing for authentication using the information, said terminal comprising:

a download section that downloads an application; and
a TRM access library section that performs processing for application authentication on condition that the authentication module authenticates the TRM access library section itself, wherein
said authentication module comprises:

a TRM section that holds a TRM access library section authentication information, which is information for authenticating said TRM access library section, in said tamper-resistant region; and
a TRM access library section authenticating section that perform authentication for said TRM access library section based on the TRM access library section authentication information.

39. An application authentication system that comprises a primary equipment and an authentication module, wherein
the primary equipment has an application storage section that stores an application, and
the authentication module has a TRM section that holds information for an authentication processing of the application in a tamper-resistant region.

40. An application authentication system that comprises a primary equipment and an authentication module, wherein
the primary equipment has:

an application storage section that stores an application; and
a TRM access library section that performs a processing for application authentication on condition that the primary equipment itself is authenticated by the authentication module, and
the authentication module has:

a TRM section that holds TRM access library section authentication information, which is information for authenticating the TRM access library section, in a tamper-resistant region; and
a TRM access library section authenticating section that performs authentication for the TRM access library section of the primary equipment based on the TRM access library section authentication information.

41. An application authentication system that comprises (N+1) pieces of equipment, which is formed by connecting a first equipment through an (N+1)th equipment in series, wherein
the first equipment has:

a TRM section that holds authentication information, which is information for authenticating

a second equipment, in a tamper-resistant region; and
a first authentication processing section that performs authentication for the second equipment based on said authentication information,
an i-th equipment, when any one of the second equipment to an N-th equipment is set to be said i-th equipment, has:

an i-th authentication processing section; and
the i-th authentication processing section performs authentication for an (i+1)th equipment on condition that the i-th authentication processing section itself is authenticated by an (i-1)th authentication processing section, and
the (N+1)th equipment has:

an application storage section that stores an application; and
an (N+1)th authentication processing section that performs a processing for authenticating said application on condition that the (N+1)th equipment itself is authenticated by an N-th authentication processing section.

42. The application authentication system according to Claim 41, wherein

said i-th equipment has an i-th authentication information obtaining section that obtains authentication information for authenticating the (i+1)th equipment, and

said i-th authentication information obtaining section, when the i-th equipment has an authentication information storage region that is a region storing the authentication information, obtains said authentication information from the authentication information storage region, and obtains said authentication information from a TRM section via the equipment from the second equipment to an (i-1)th equipment when said authentication information is stored in the TRM section of the first equipment.

FIG. 1

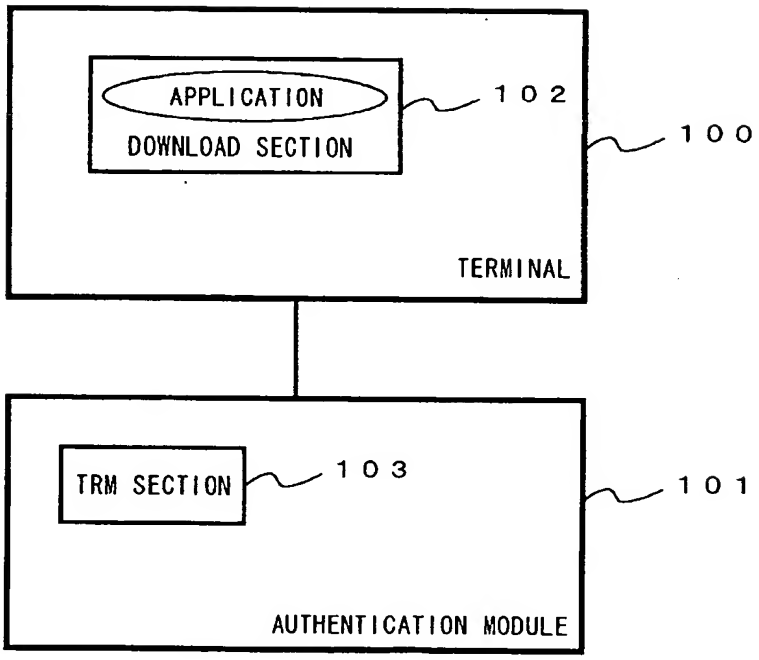

APPLICATION
DOWNLOAD SECTION
102
100
TERMINAL
TRM SECTION
103
101
AUTHENTICATION MODULE

FIG. 2

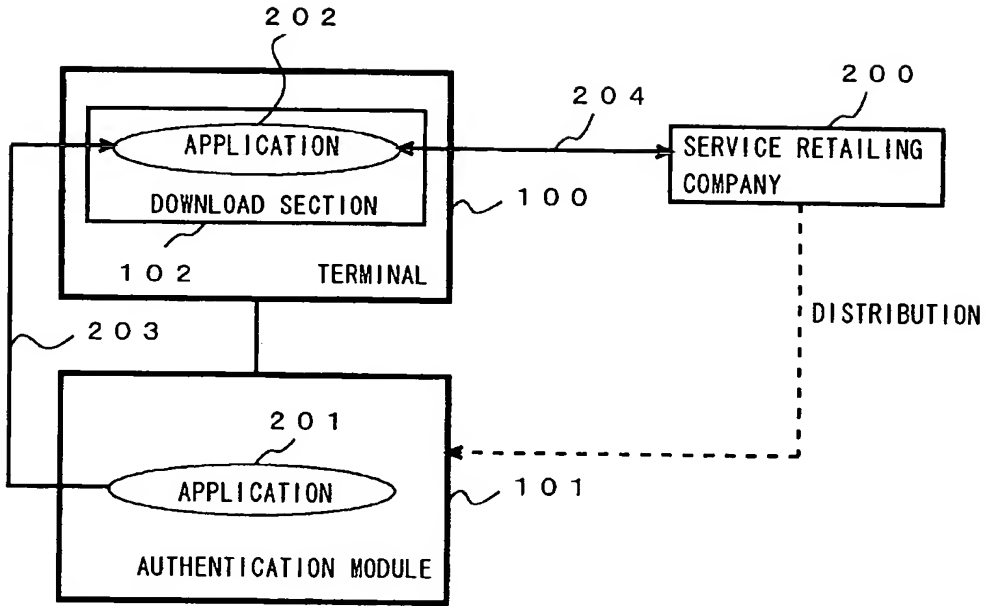

202
200
204
APPLICATION
SERVICE RETAILING COMPANY
DOWNLOAD SECTION
100
102
TERMINAL
DISTRIBUTION
203
201
APPLICATION
101
AUTHENTICATION MODULE

FIG. 3

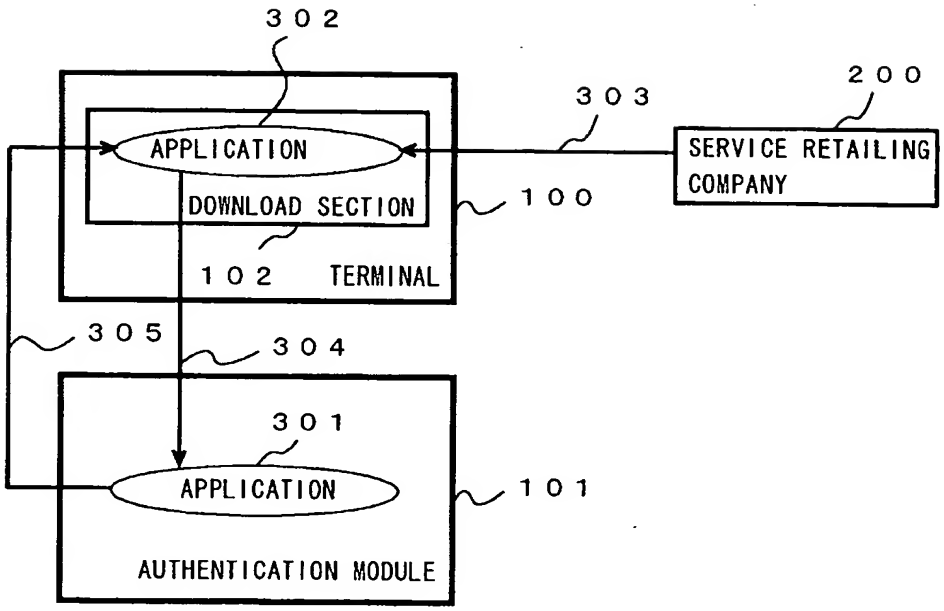

302
200
303
APPLICATION
SERVICE RETAILING COMPANY
DOWNLOAD SECTION
100
102 TERMINAL
305
304
301
APPLICATION
101
AUTHENTICATION MODULE

FIG. 4

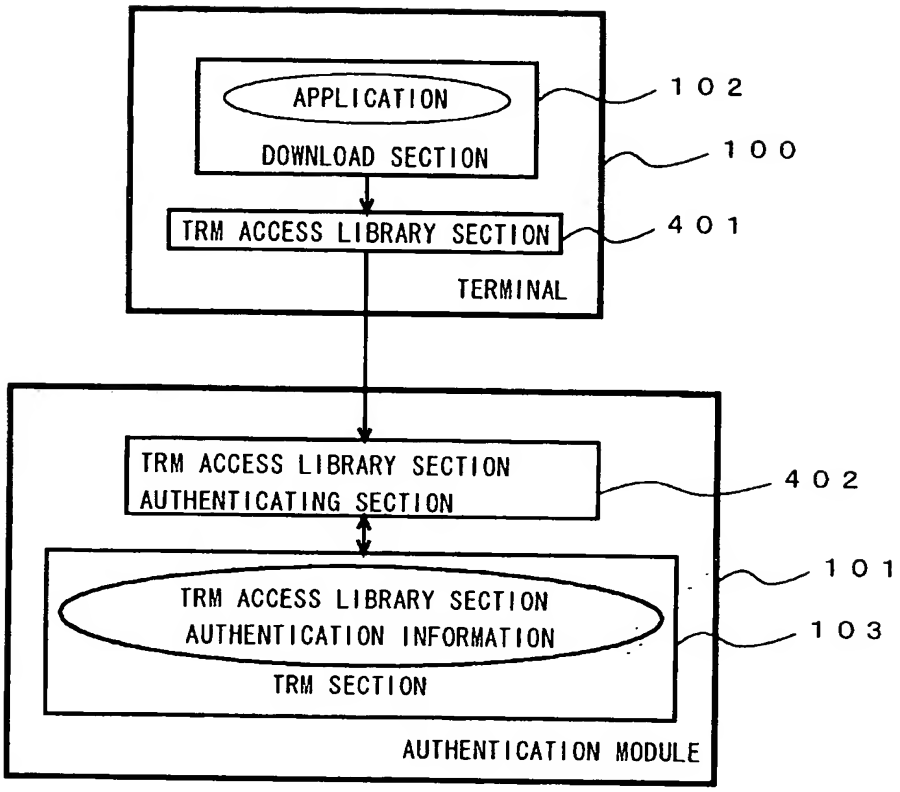

APPLICATION
DOWNLOAD SECTION
102
100
TRM ACCESS LIBRARY SECTION
401
TERMINAL
TRM ACCESS LIBRARY SECTION
AUTHENTICATING SECTION
402
TRM ACCESS LIBRARY SECTION
AUTHENTICATION INFORMATION
101
103
TRM SECTION
AUTHENTICATION MODULE

FIG. 5

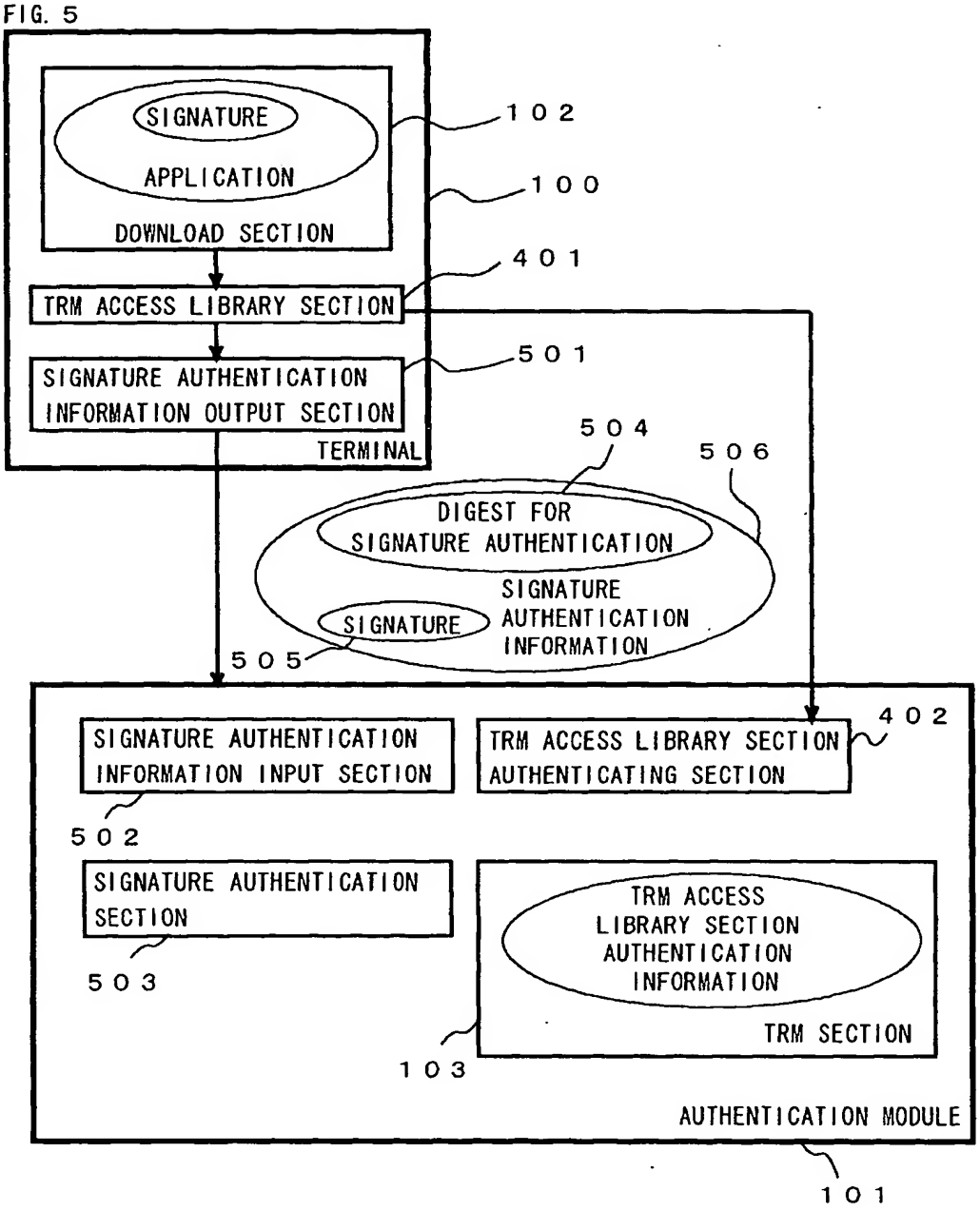

SIGNATURE
APPLICATION
DOWNLOAD SECTION
102
100
401
TRM ACCESS LIBRARY SECTION
501
SIGNATURE AUTHENTICATION INFORMATION OUTPUT SECTION
TERMINAL
504
506
DIGEST FOR SIGNATURE AUTHENTICATION
SIGNATURE
SIGNATURE AUTHENTICATION INFORMATION
505
402
SIGNATURE AUTHENTICATION INFORMATION INPUT SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
502
SIGNATURE AUTHENTICATION SECTION
503
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
TRM SECTION
103
AUTHENTICATION MODULE
101

FIG. 6

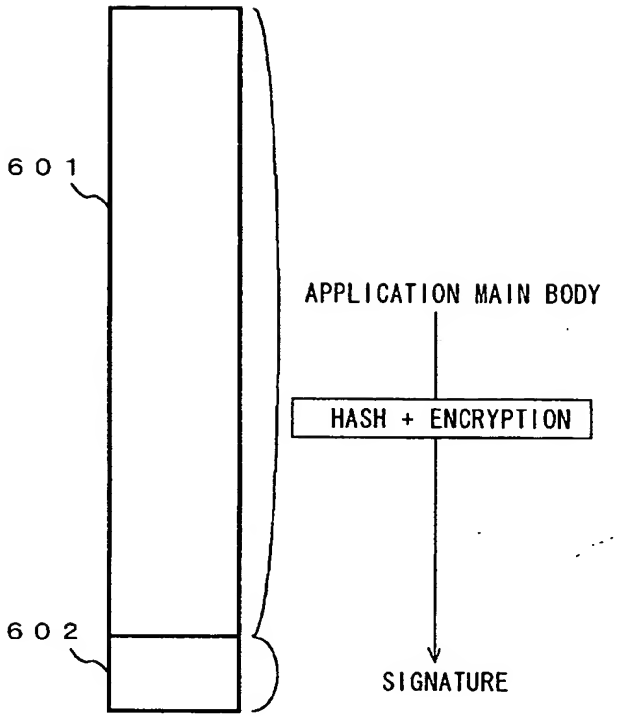


FIG. 7

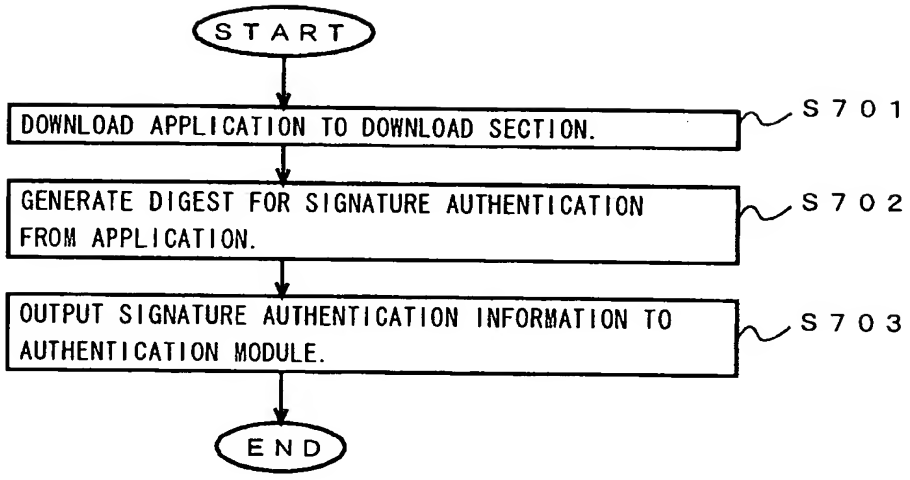

START
DOWNLOAD APPLICATION TO DOWNLOAD SECTION.
S701
GENERATE DIGEST FOR SIGNATURE AUTHENTICATION FROM APPLICATION.
S702
OUTPUT SIGNATURE AUTHENTICATION INFORMATION TO AUTHENTICATION MODULE.
S703
END

FIG. 8

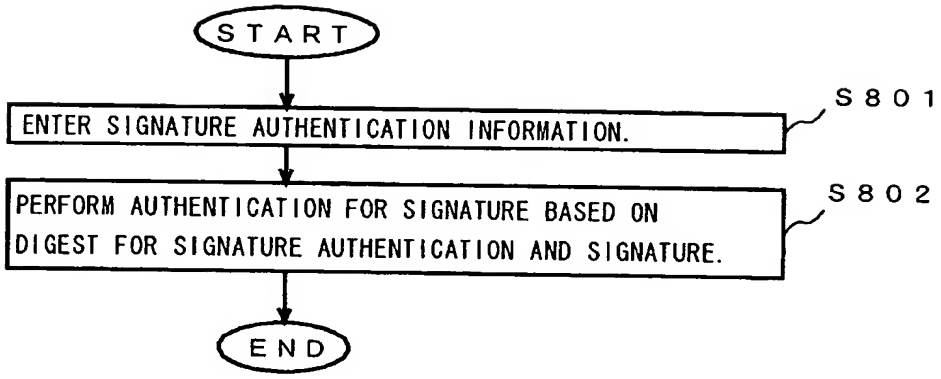

START
ENTER SIGNATURE AUTHENTICATION INFORMATION.
S801
PERFORM AUTHENTICATION FOR SIGNATURE BASED ON DIGEST FOR SIGNATURE AUTHENTICATION AND SIGNATURE.
S802
END

FIG. 9

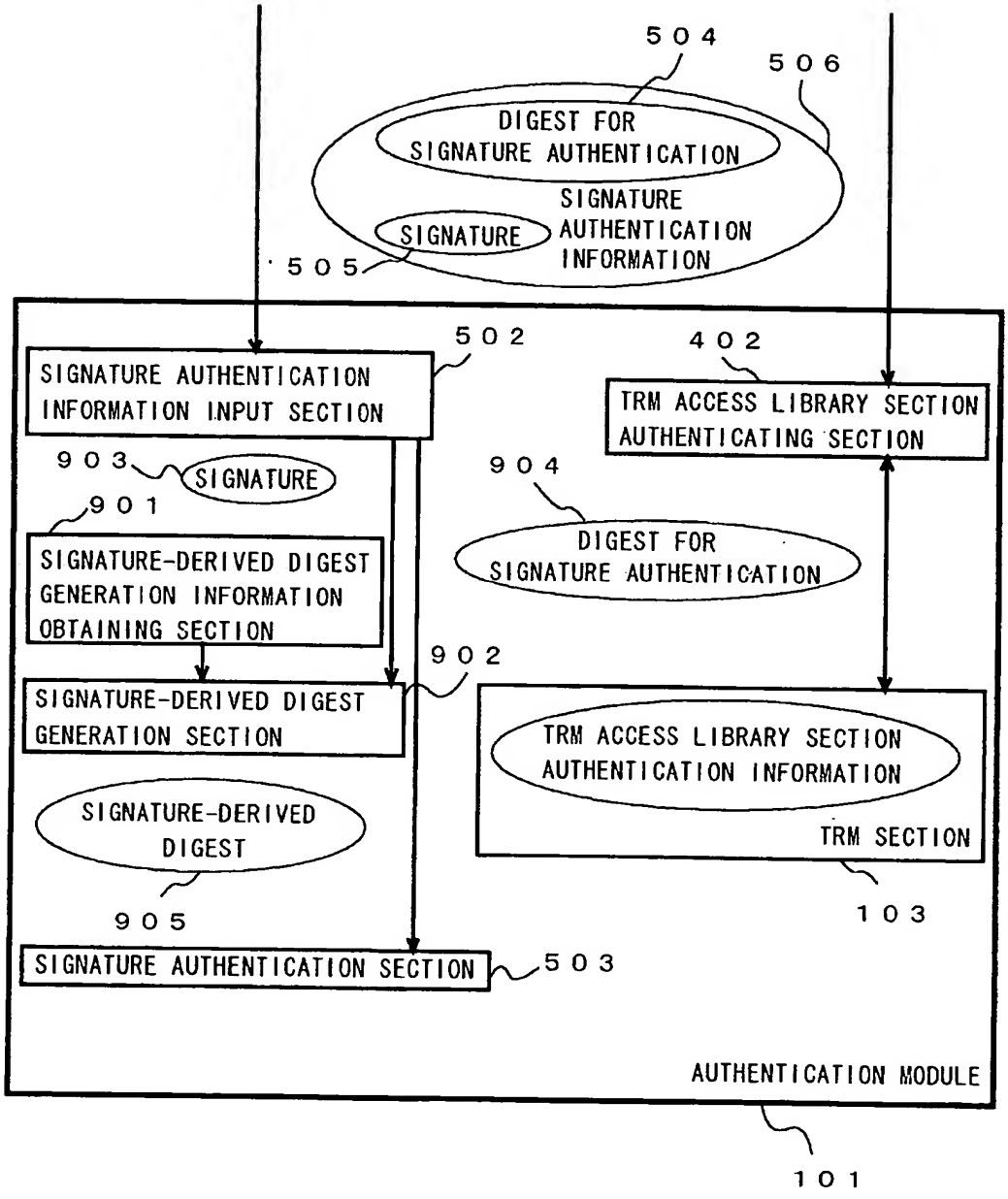

504
506
DIGEST FOR SIGNATURE AUTHENTICATION
SIGNATURE AUTHENTICATION INFORMATION
SIGNATURE
505
502
SIGNATURE AUTHENTICATION INFORMATION INPUT SECTION
402
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
903
SIGNATURE
901
SIGNATURE-DERIVED DIGEST GENERATION INFORMATION OBTAINING SECTION
904
DIGEST FOR SIGNATURE AUTHENTICATION
902
SIGNATURE-DERIVED DIGEST GENERATION SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
TRM SECTION
103
SIGNATURE-DERIVED DIGEST
905
SIGNATURE AUTHENTICATION SECTION
503
AUTHENTICATION MODULE
101

FIG. 10

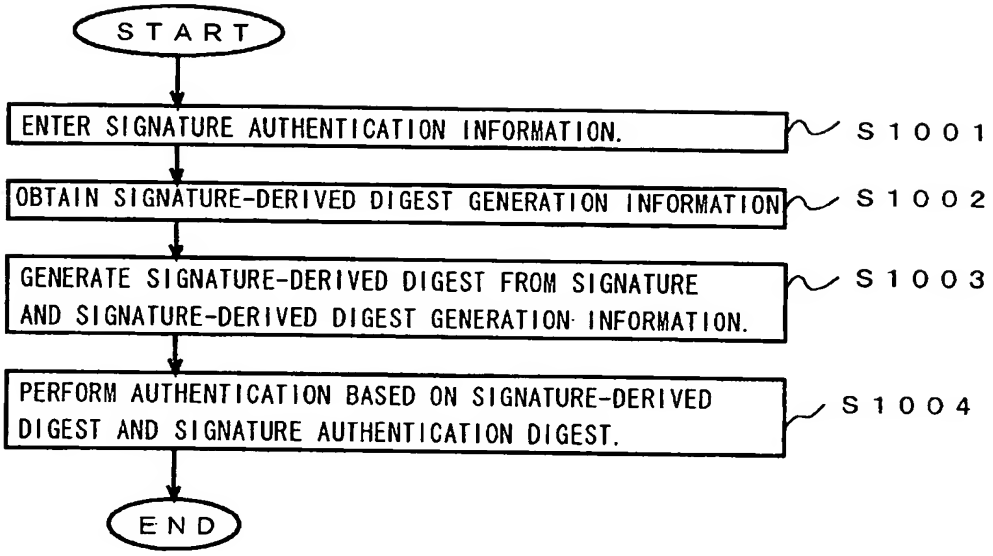

START
ENTER SIGNATURE AUTHENTICATION INFORMATION.
S1001
OBTAIN SIGNATURE-DERIVED DIGEST GENERATION INFORMATION
S1002
GENERATE SIGNATURE-DERIVED DIGEST FROM SIGNATURE AND SIGNATURE-DERIVED DIGEST GENERATION INFORMATION.
S1003
PERFORM AUTHENTICATION BASED ON SIGNATURE-DERIVED DIGEST AND SIGNATURE AUTHENTICATION DIGEST.
S1004
END

FIG. 11

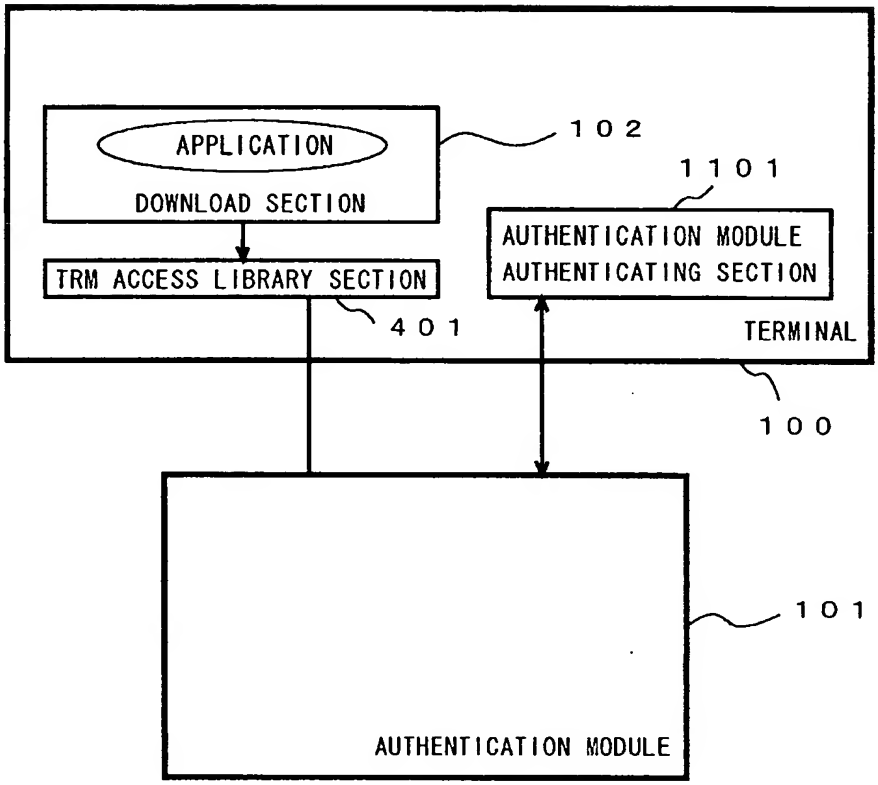

APPLICATION
DOWNLOAD SECTION
102
1101
AUTHENTICATION MODULE
AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION
401
TERMINAL
100
101
AUTHENTICATION MODULE

FIG. 12

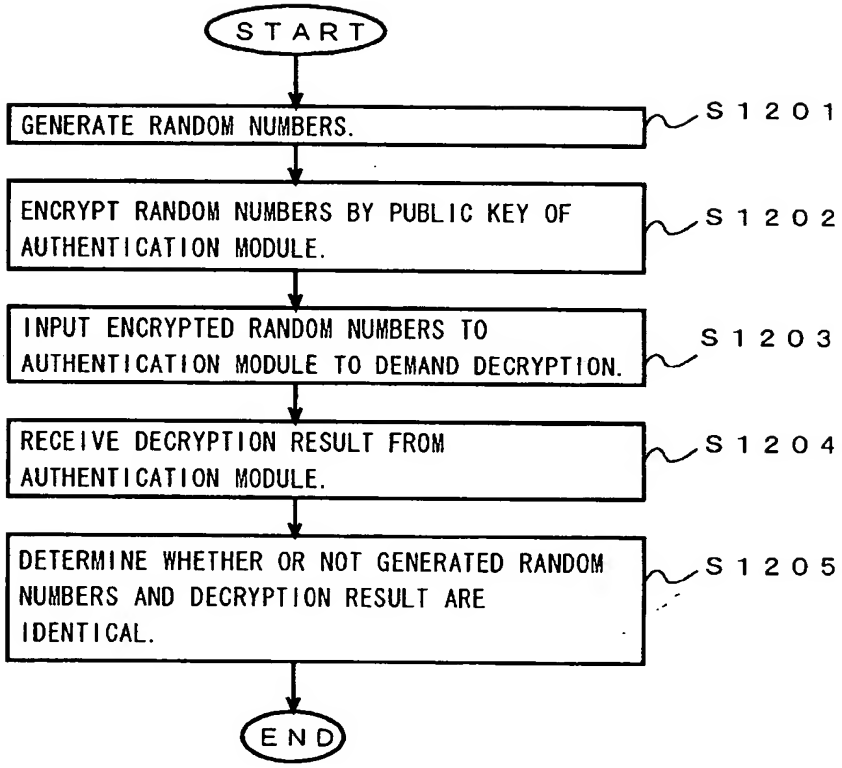

START
GENERATE RANDOM NUMBERS.
S1201
ENCRYPT RANDOM NUMBERS BY PUBLIC KEY OF AUTHENTICATION MODULE.
S1202
INPUT ENCRYPTED RANDOM NUMBERS TO AUTHENTICATION MODULE TO DEMAND DECRYPTION.
S1203
RECEIVE DECRYPTION RESULT FROM AUTHENTICATION MODULE.
S1204
DETERMINE WHETHER OR NOT GENERATED RANDOM NUMBERS AND DECRYPTION RESULT ARE IDENTICAL.
S1205
END

FIG. 13

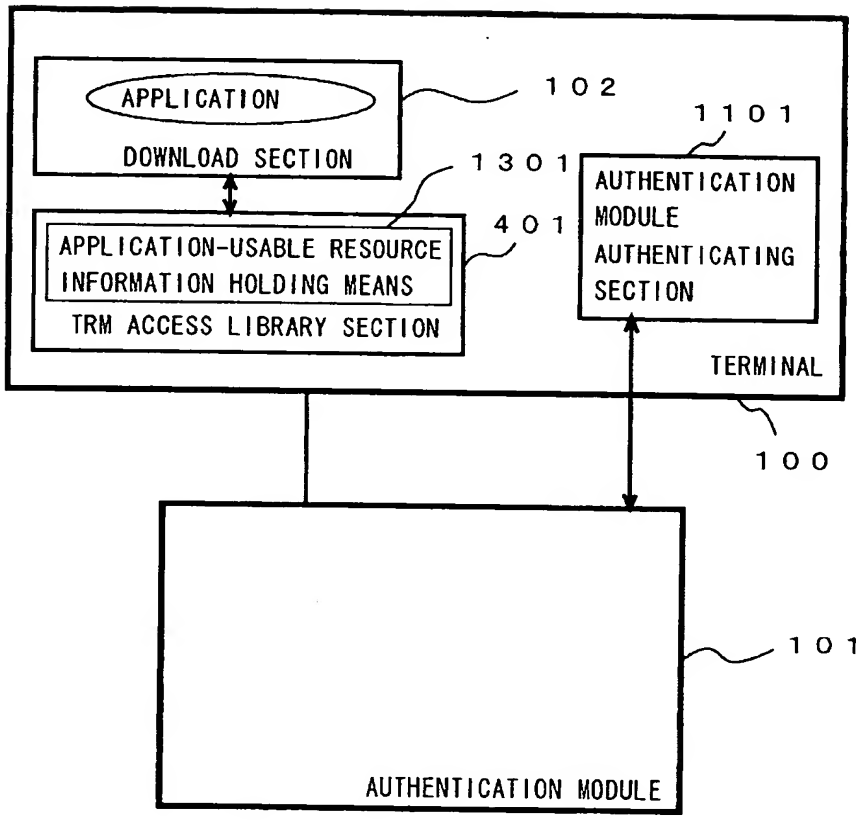

APPLICATION
DOWNLOAD SECTION
102
1101
1301
AUTHENTICATION MODULE AUTHENTICATING SECTION
401
APPLICATION-USABLE RESOURCE INFORMATION HOLDING MEANS
TRM ACCESS LIBRARY SECTION
TERMINAL
100
101
AUTHENTICATION MODULE

FIG. 14

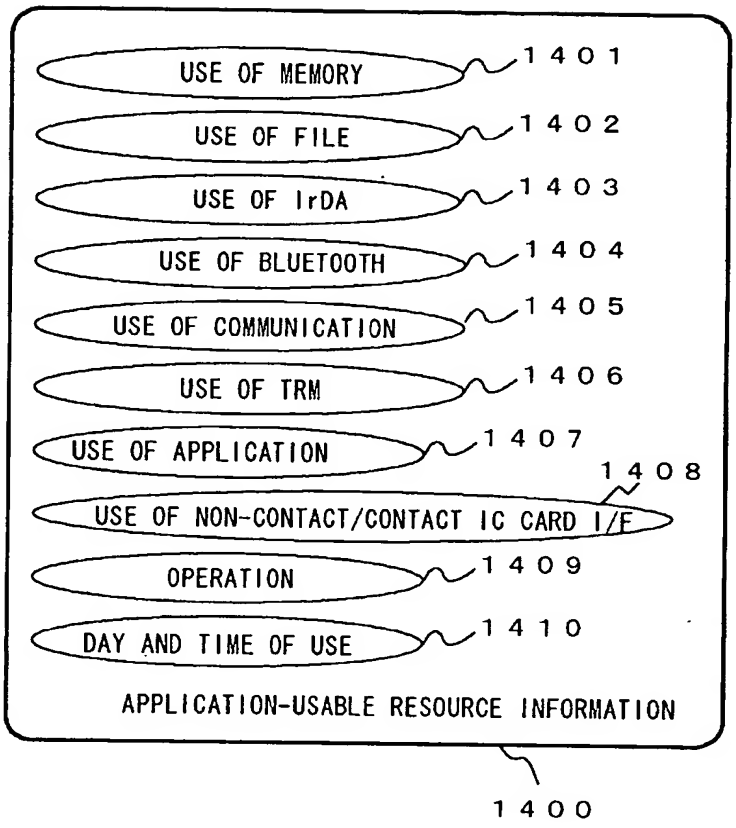

USE OF MEMORY
1401
USE OF FILE
1402
USE OF IrDA
1403
USE OF BLUETOOTH
1404
USE OF COMMUNICATION
1405
USE OF TRM
1406
USE OF APPLICATION
1407
1408
USE OF NON-CONTACT/CONTACT IC CARD I/F
OPERATION
1409
DAY AND TIME OF USE
1410
APPLICATION-USABLE RESOURCE INFORMATION
1400

FIG. 15

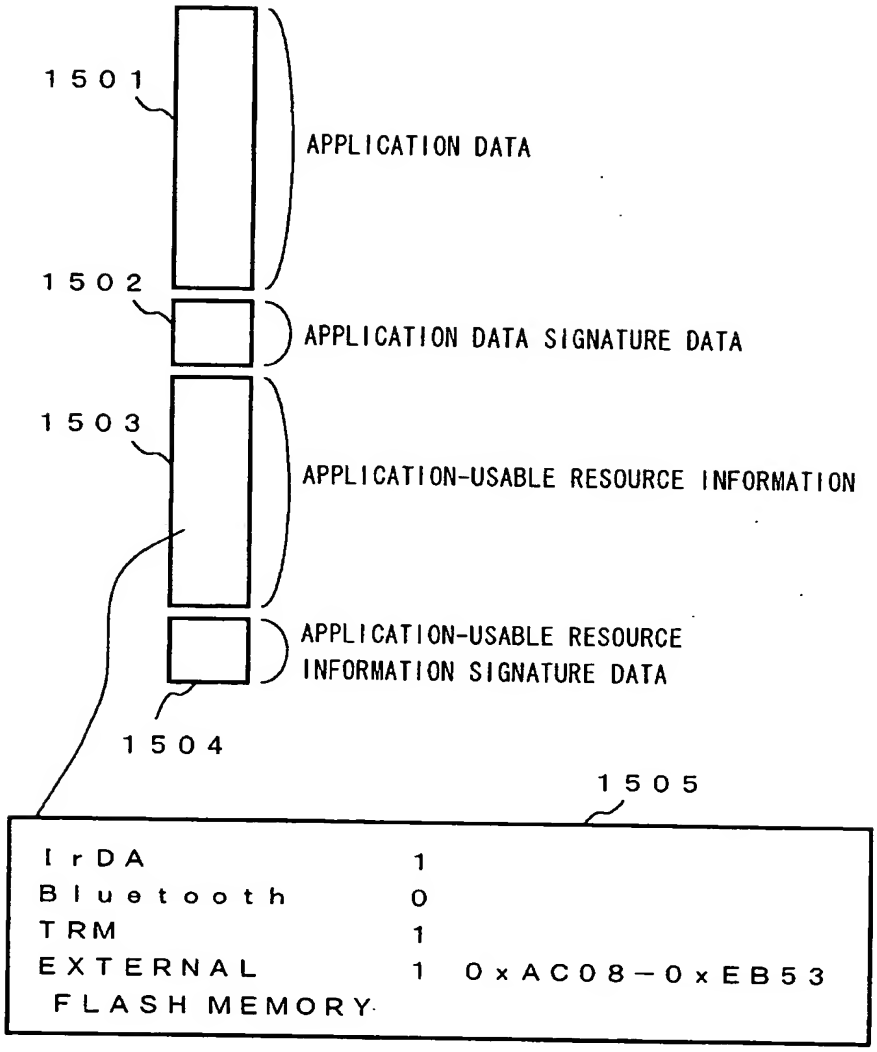

1501
APPLICATION DATA
1502
APPLICATION DATA SIGNATURE DATA
1503
APPLICATION-USABLE RESOURCE INFORMATION
APPLICATION-USABLE RESOURCE INFORMATION SIGNATURE DATA
1504
1505
IrDA 1
Bluetooth 0
TRM 1
EXTERNAL FLASH MEMORY 1 0xAC08−0xEB53

FIG. 16

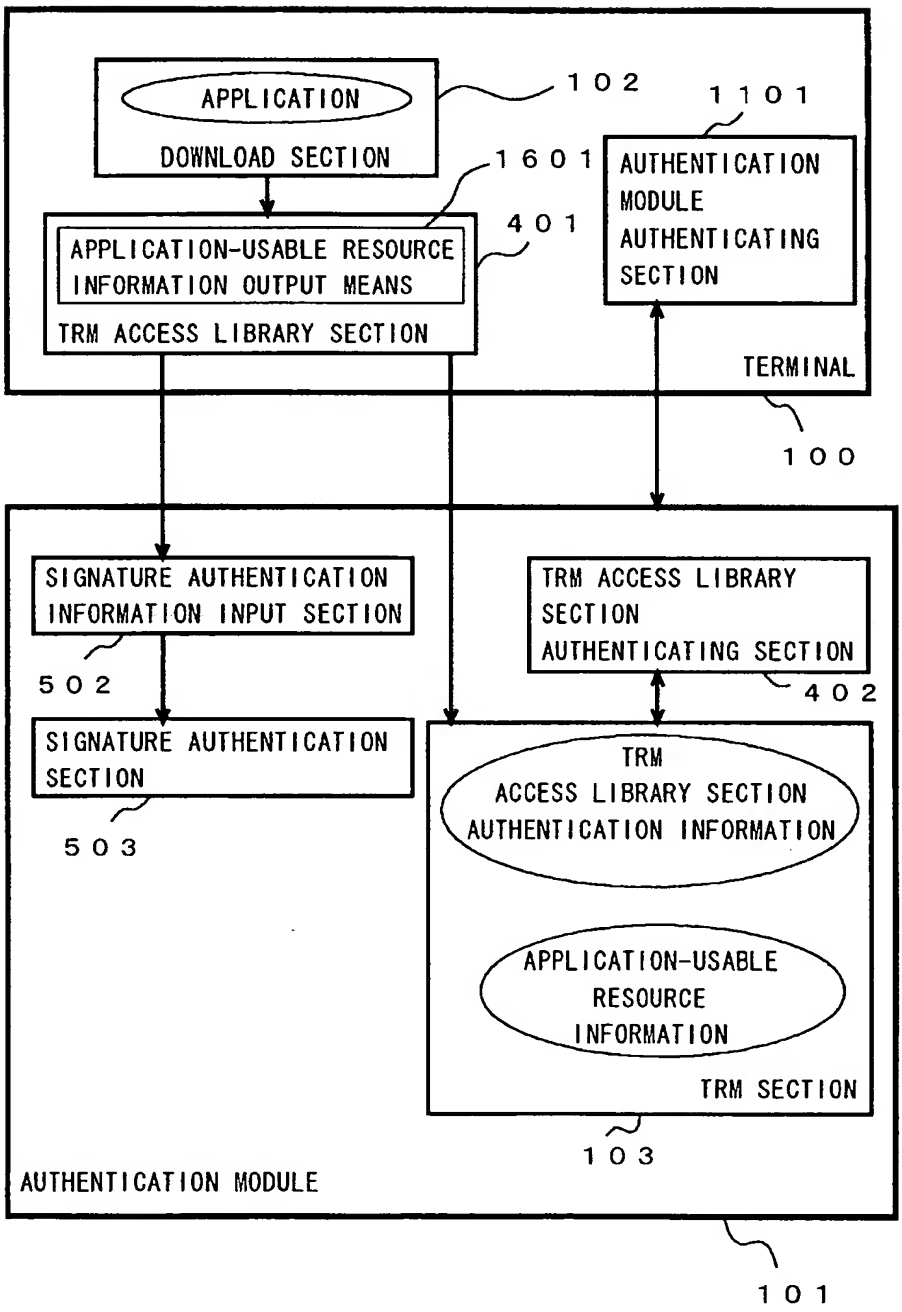

APPLICATION
DOWNLOAD SECTION
102
1101
1601
AUTHENTICATION MODULE AUTHENTICATING SECTION
401
APPLICATION-USABLE RESOURCE INFORMATION OUTPUT MEANS
TRM ACCESS LIBRARY SECTION
TERMINAL
100
SIGNATURE AUTHENTICATION INFORMATION INPUT SECTION
502
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
402
SIGNATURE AUTHENTICATION SECTION
503
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
APPLICATION-USABLE RESOURCE INFORMATION
TRM SECTION
103
AUTHENTICATION MODULE
101

FIG. 17

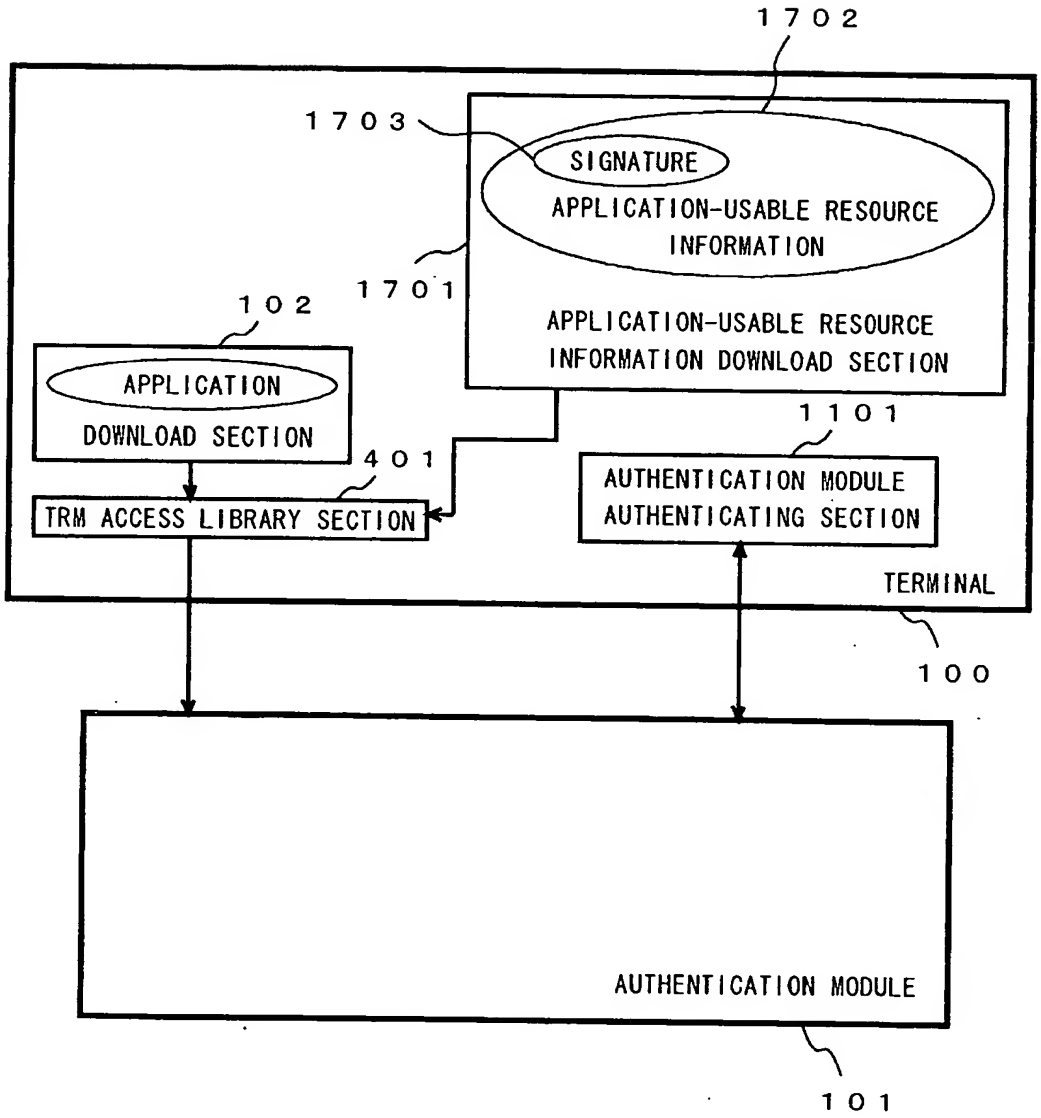

1702
1703
SIGNATURE
APPLICATION-USABLE RESOURCE INFORMATION
1701
APPLICATION-USABLE RESOURCE INFORMATION DOWNLOAD SECTION
102
APPLICATION DOWNLOAD SECTION
1101
401
AUTHENTICATION MODULE AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION
TERMINAL
100
AUTHENTICATION MODULE
101

FIG. 18

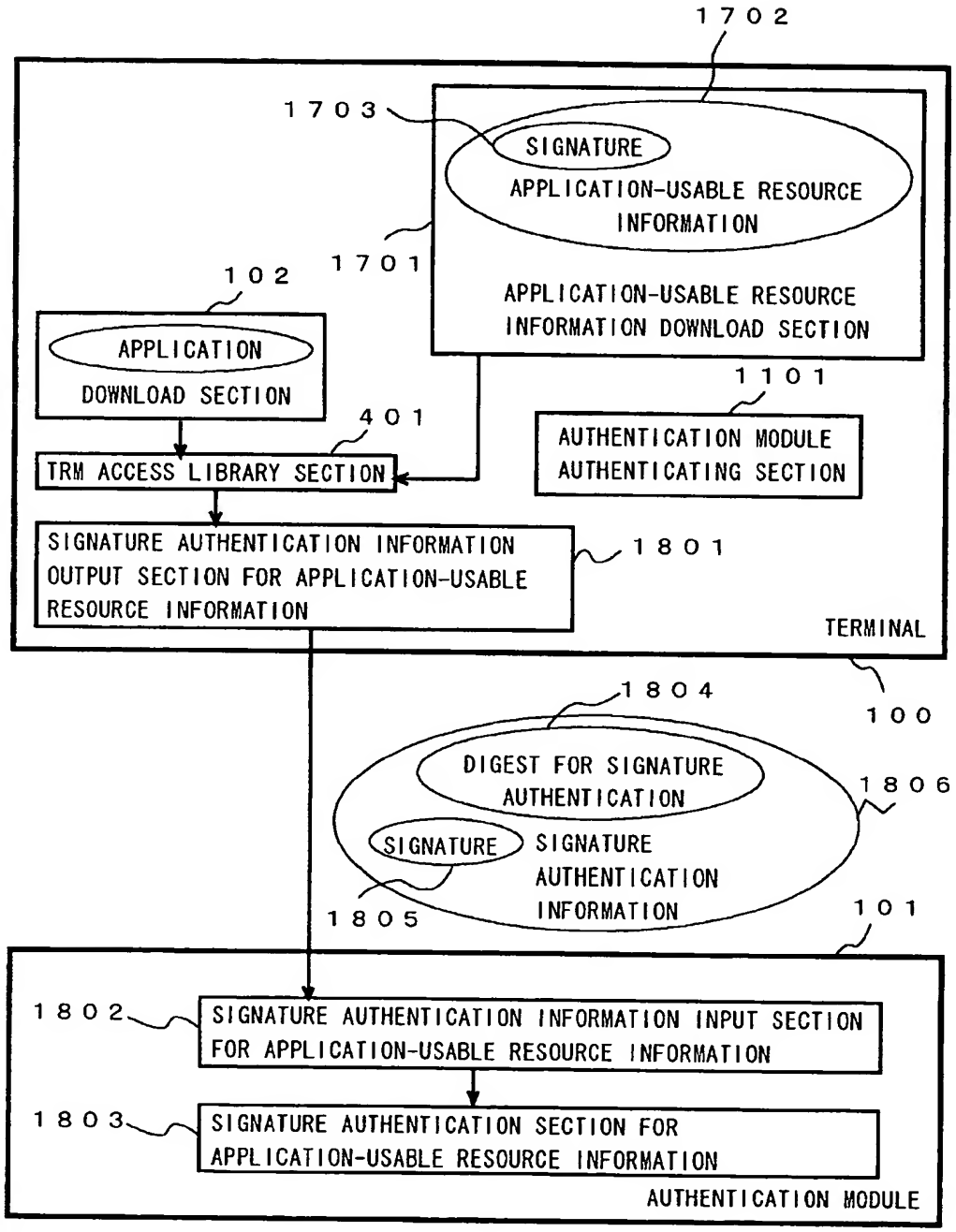

1702
1703
SIGNATURE
APPLICATION-USABLE RESOURCE INFORMATION
1701
APPLICATION-USABLE RESOURCE INFORMATION DOWNLOAD SECTION
102
APPLICATION DOWNLOAD SECTION
1101
AUTHENTICATION MODULE AUTHENTICATING SECTION
401
TRM ACCESS LIBRARY SECTION
SIGNATURE AUTHENTICATION INFORMATION OUTPUT SECTION FOR APPLICATION-USABLE RESOURCE INFORMATION
1801
TERMINAL
100
1804
DIGEST FOR SIGNATURE AUTHENTICATION
1806
SIGNATURE
SIGNATURE AUTHENTICATION INFORMATION
1805
101
1802
SIGNATURE AUTHENTICATION INFORMATION INPUT SECTION FOR APPLICATION-USABLE RESOURCE INFORMATION
1803
SIGNATURE AUTHENTICATION SECTION FOR APPLICATION-USABLE RESOURCE INFORMATION
AUTHENTICATION MODULE

FIG. 19

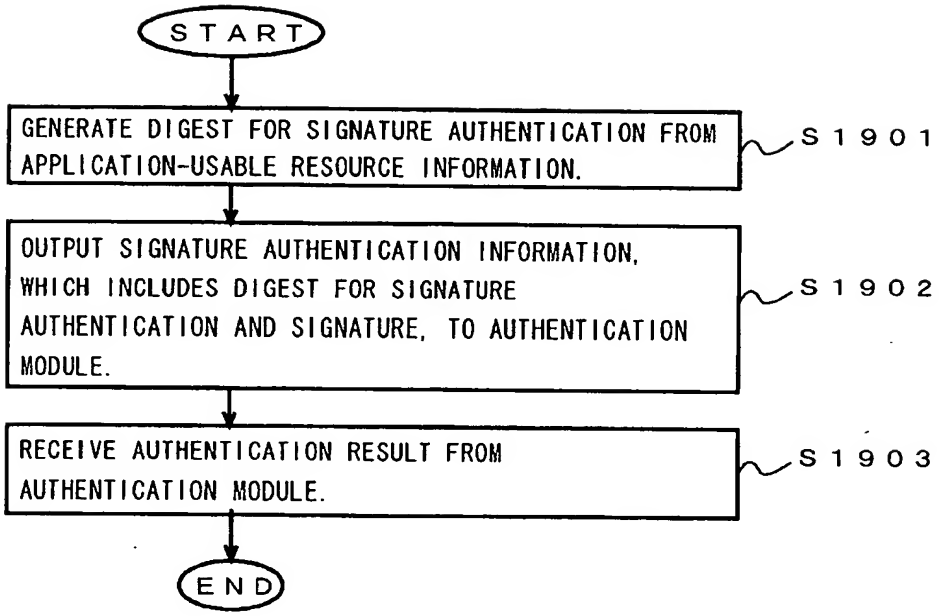

START
GENERATE DIGEST FOR SIGNATURE AUTHENTICATION FROM APPLICATION-USABLE RESOURCE INFORMATION.
S1901
OUTPUT SIGNATURE AUTHENTICATION INFORMATION, WHICH INCLUDES DIGEST FOR SIGNATURE AUTHENTICATION AND SIGNATURE, TO AUTHENTICATION MODULE.
S1902
RECEIVE AUTHENTICATION RESULT FROM AUTHENTICATION MODULE.
S1903
END

FIG. 20

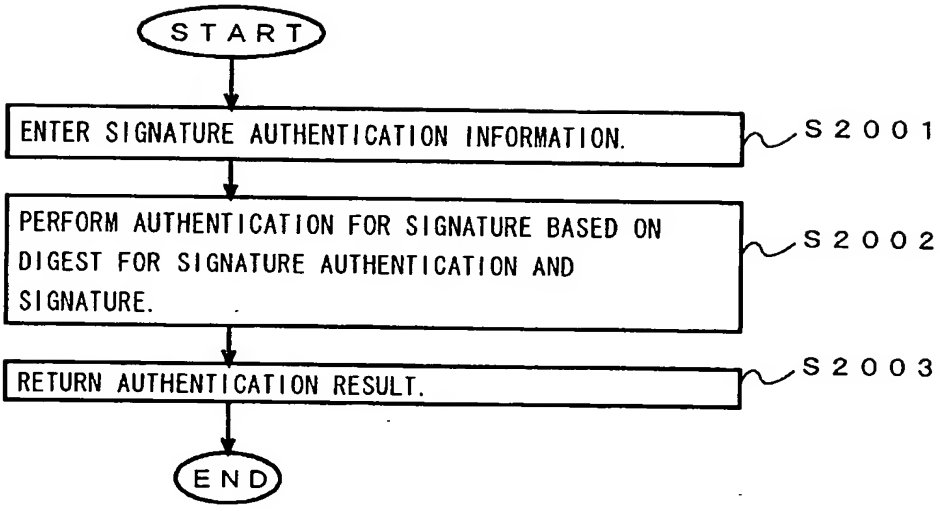

START
ENTER SIGNATURE AUTHENTICATION INFORMATION.
S2001
PERFORM AUTHENTICATION FOR SIGNATURE BASED ON DIGEST FOR SIGNATURE AUTHENTICATION AND SIGNATURE.
S2002
RETURN AUTHENTICATION RESULT.
S2003
END

FIG. 21

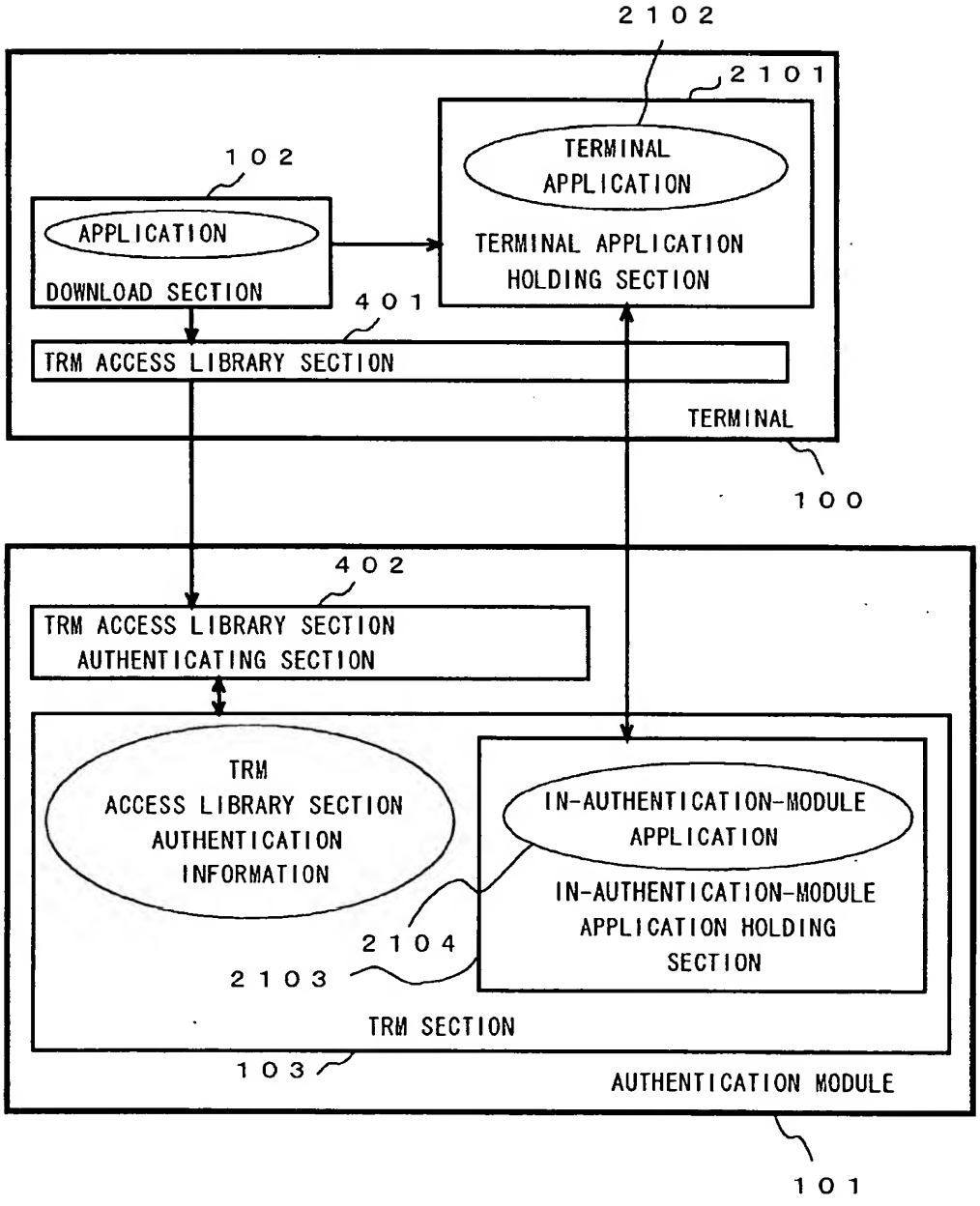

2102
2101
TERMINAL APPLICATION
102
APPLICATION
DOWNLOAD SECTION
TERMINAL APPLICATION HOLDING SECTION
401
TRM ACCESS LIBRARY SECTION
TERMINAL
100
402
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
IN-AUTHENTICATION-MODULE APPLICATION
IN-AUTHENTICATION-MODULE APPLICATION HOLDING SECTION
2104
2103
TRM SECTION
103
AUTHENTICATION MODULE
101

FIG. 22

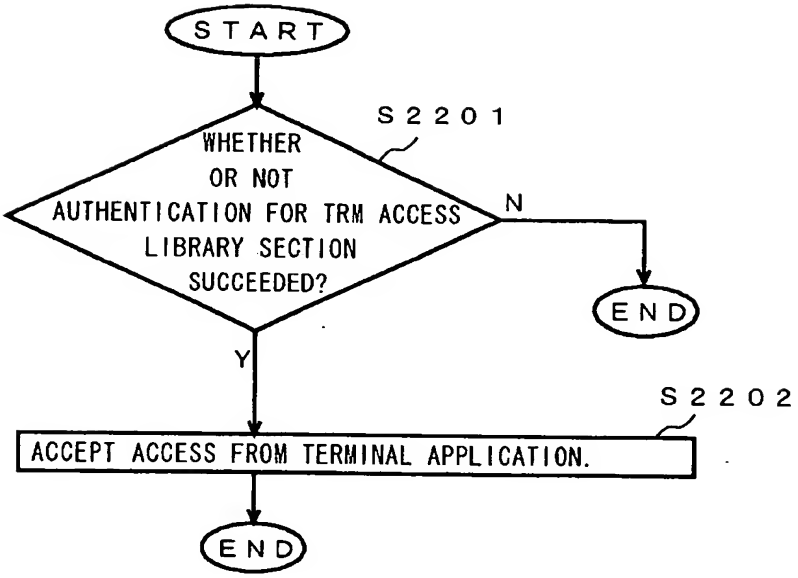

START
S2201
WHETHER OR NOT AUTHENTICATION FOR TRM ACCESS LIBRARY SECTION SUCCEEDED?
N
END
Y
S2202
ACCEPT ACCESS FROM TERMINAL APPLICATION.
END

FIG. 23

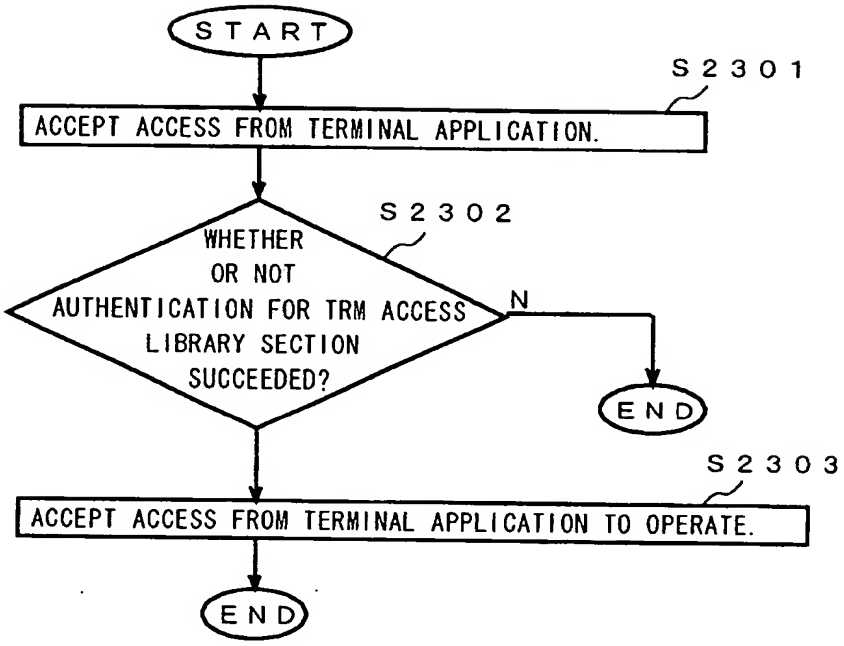

START
S2301
ACCEPT ACCESS FROM TERMINAL APPLICATION.
S2302
WHETHER OR NOT AUTHENTICATION FOR TRM ACCESS LIBRARY SECTION SUCCEEDED?
N
END
S2303
ACCEPT ACCESS FROM TERMINAL APPLICATION TO OPERATE.
END

FIG. 24

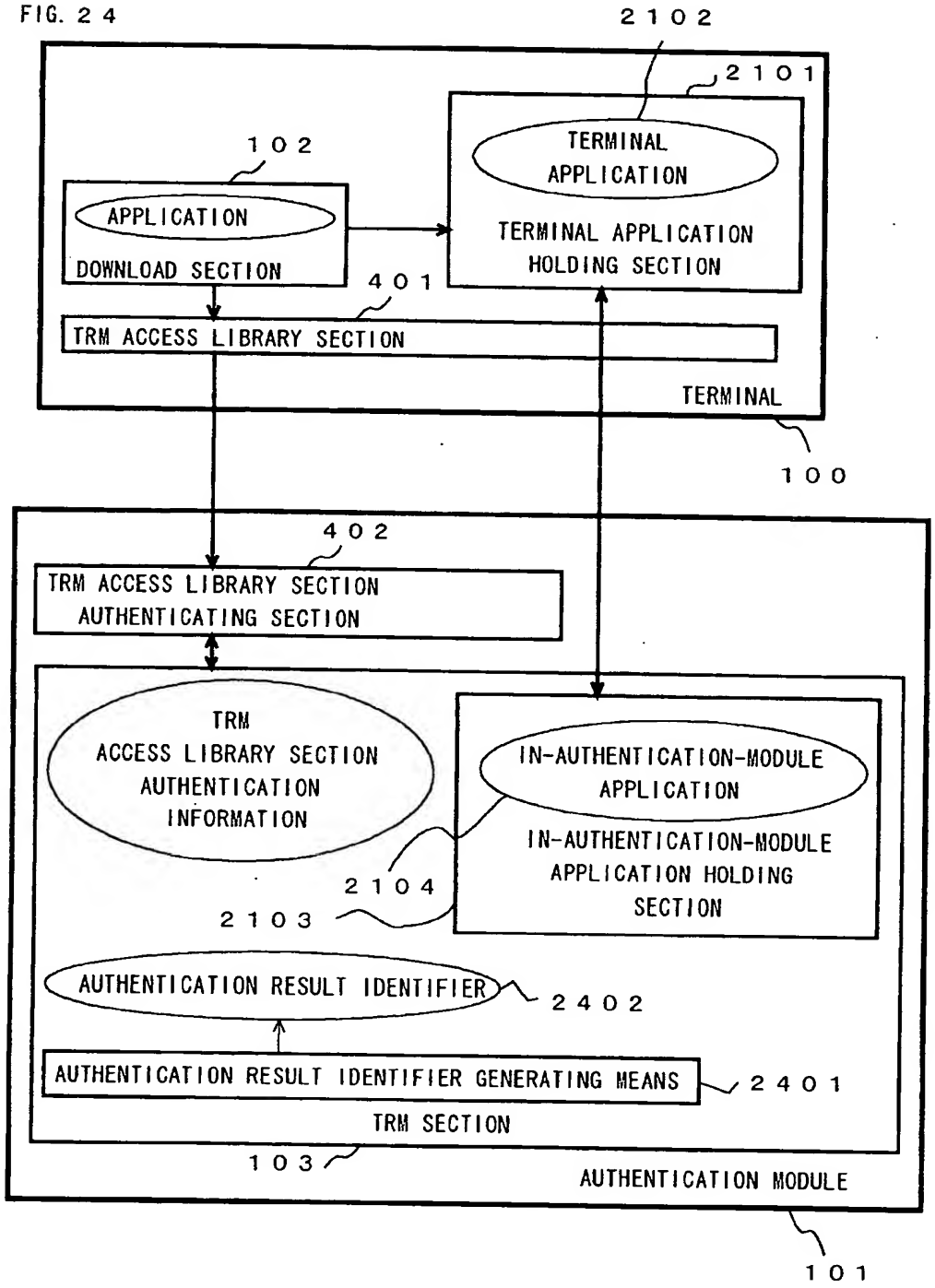

2102
2101
TERMINAL APPLICATION
102
APPLICATION
DOWNLOAD SECTION
TERMINAL APPLICATION HOLDING SECTION
401
TRM ACCESS LIBRARY SECTION
TERMINAL
100
402
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
IN-AUTHENTICATION-MODULE APPLICATION
IN-AUTHENTICATION-MODULE APPLICATION HOLDING SECTION
2104
2103
AUTHENTICATION RESULT IDENTIFIER
2402
AUTHENTICATION RESULT IDENTIFIER GENERATING MEANS
2401
TRM SECTION
103
AUTHENTICATION MODULE
101

FIG. 25

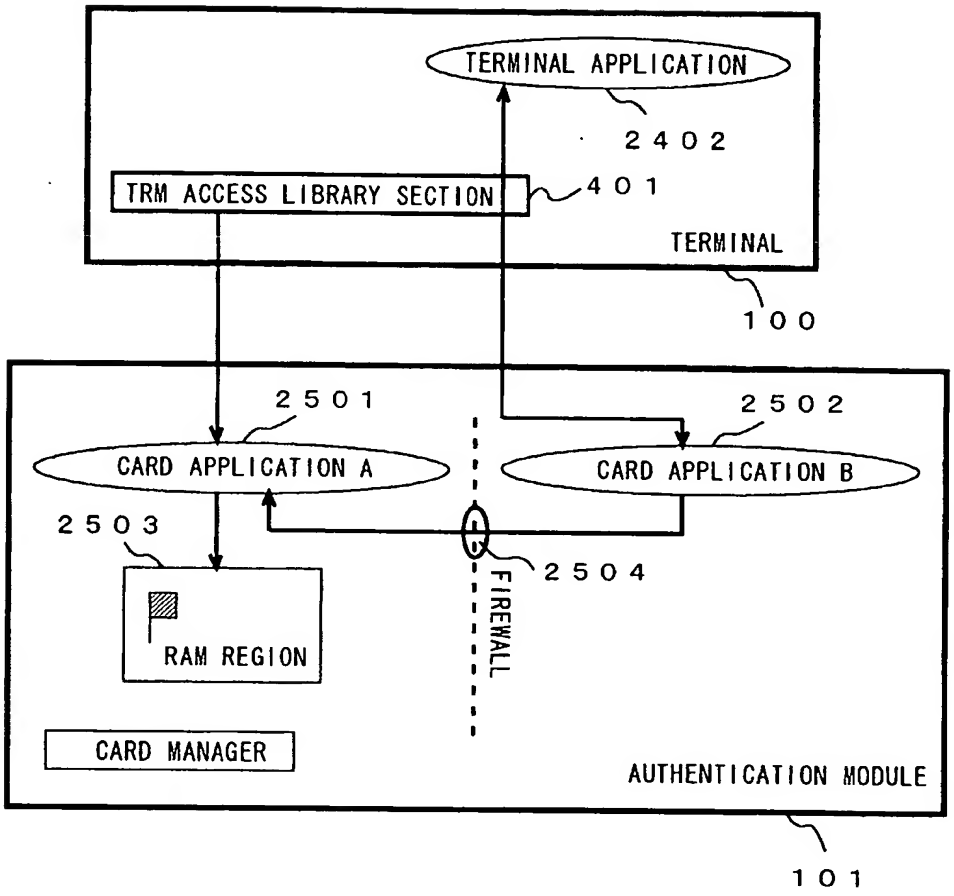

TERMINAL APPLICATION
2402
TRM ACCESS LIBRARY SECTION
401
TERMINAL
100
2501
2502
CARD APPLICATION A
CARD APPLICATION B
2503
2504
FIREWALL
RAM REGION
CARD MANAGER
AUTHENTICATION MODULE
101

FIG. 26

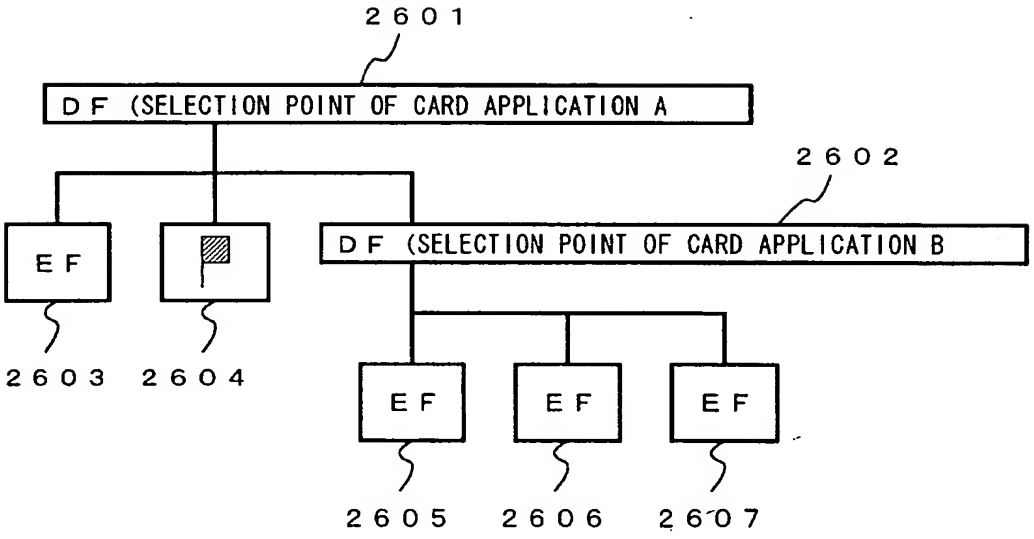

2601
DF (SELECTION POINT OF CARD APPLICATION A
2602
EF
DF (SELECTION POINT OF CARD APPLICATION B
2603
2604
EF
EF
EF
2605
2606
2607

FIG. 27

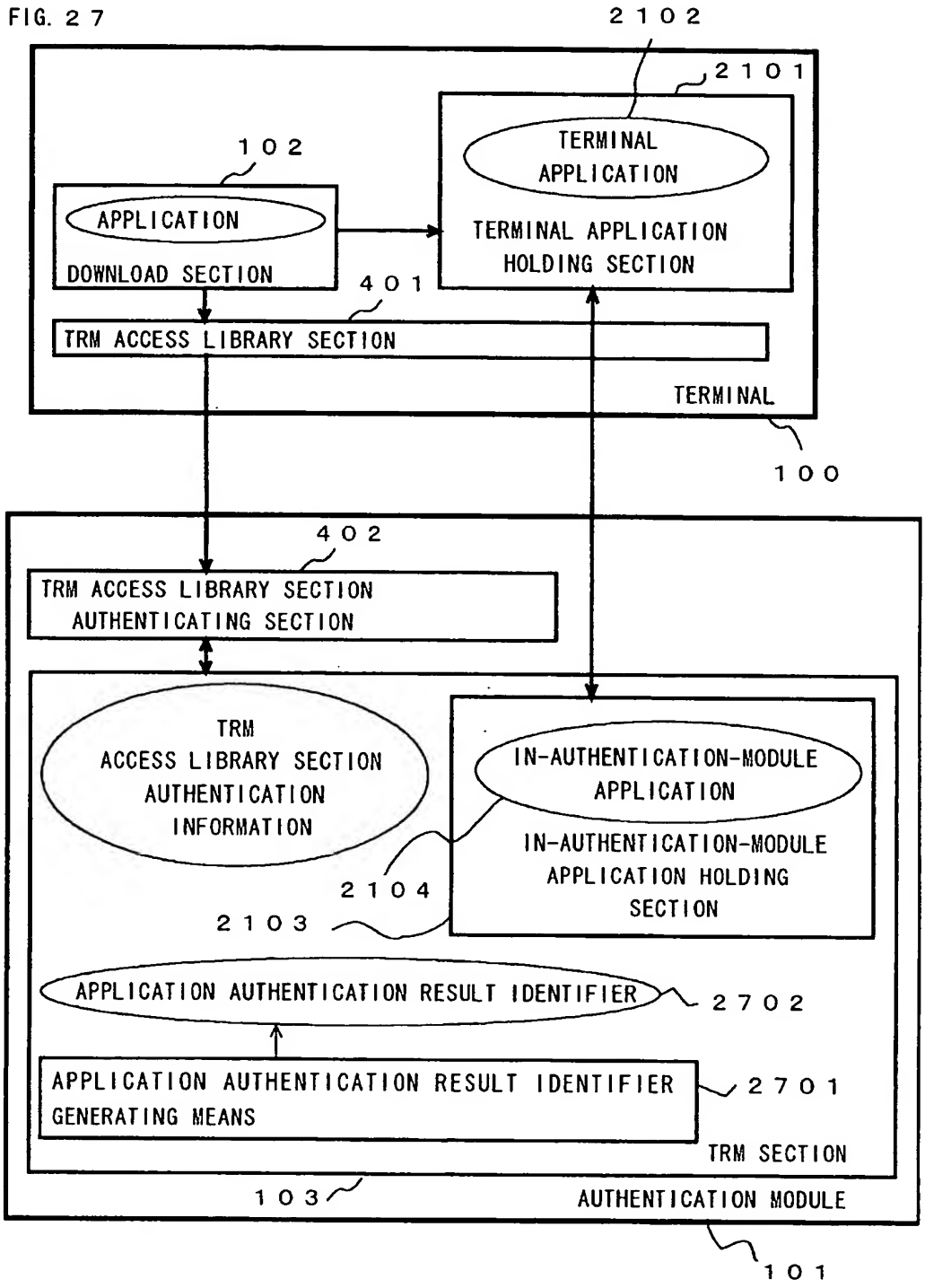

2102
2101
TERMINAL APPLICATION
102
APPLICATION
DOWNLOAD SECTION
TERMINAL APPLICATION HOLDING SECTION
401
TRM ACCESS LIBRARY SECTION
TERMINAL
100
402
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
IN-AUTHENTICATION-MODULE APPLICATION
IN-AUTHENTICATION-MODULE APPLICATION HOLDING SECTION
2104
2103
APPLICATION AUTHENTICATION RESULT IDENTIFIER
2702
APPLICATION AUTHENTICATION RESULT IDENTIFIER GENERATING MEANS
2701
TRM SECTION
103
AUTHENTICATION MODULE
101

FIG. 28

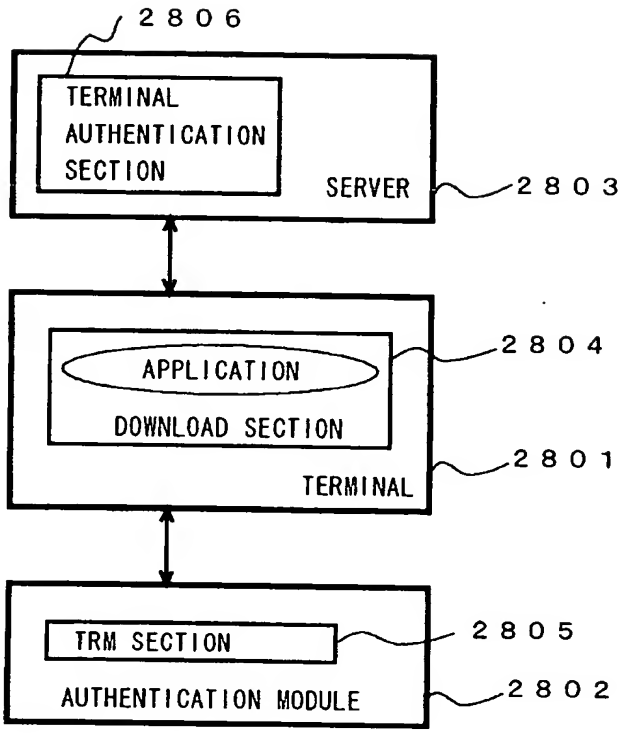

2806
TERMINAL AUTHENTICATION SECTION
SERVER
2803
APPLICATION
DOWNLOAD SECTION
2804
TERMINAL
2801
TRM SECTION
2805
AUTHENTICATION MODULE
2802

FIG. 29

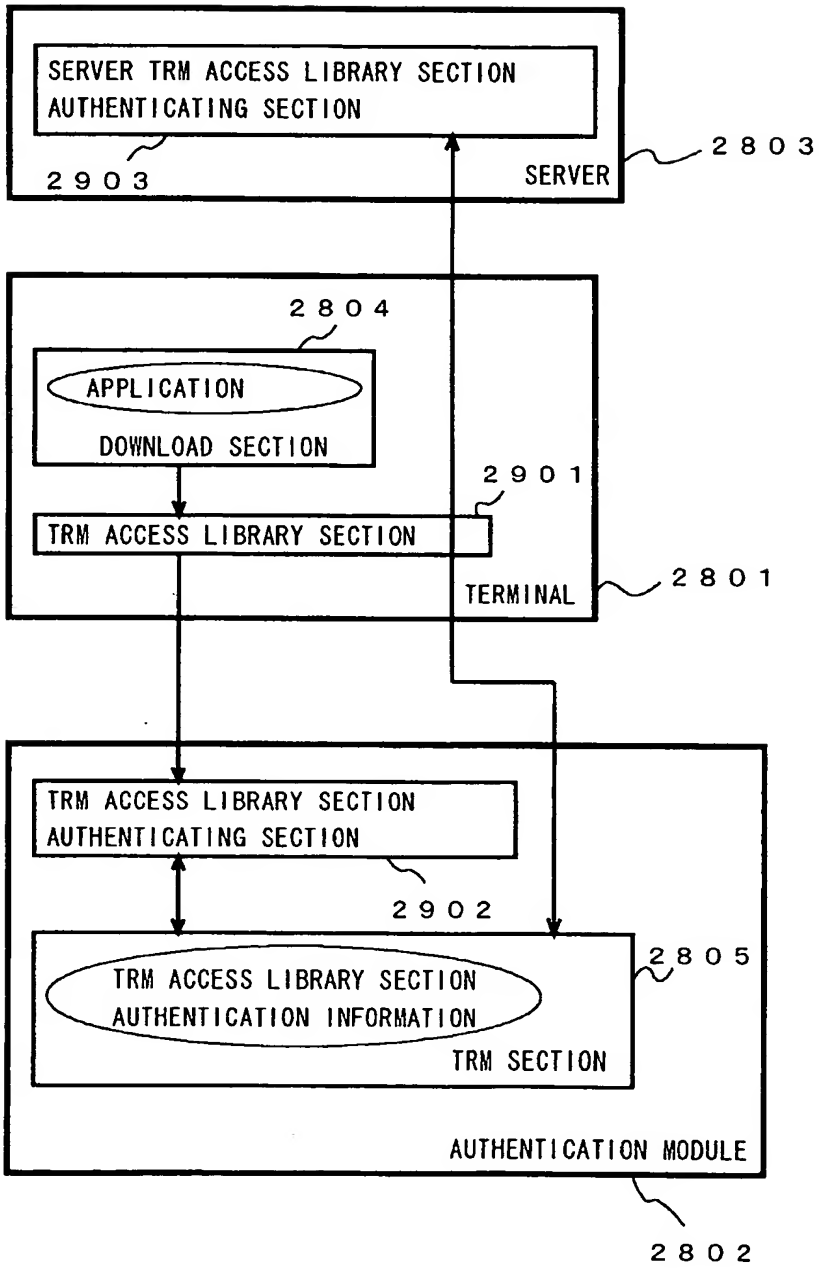

SERVER TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
2903
SERVER
2803
2804
APPLICATION DOWNLOAD SECTION
2901
TRM ACCESS LIBRARY SECTION
TERMINAL
2801
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
2902
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
TRM SECTION
2805
AUTHENTICATION MODULE
2802

FIG. 30

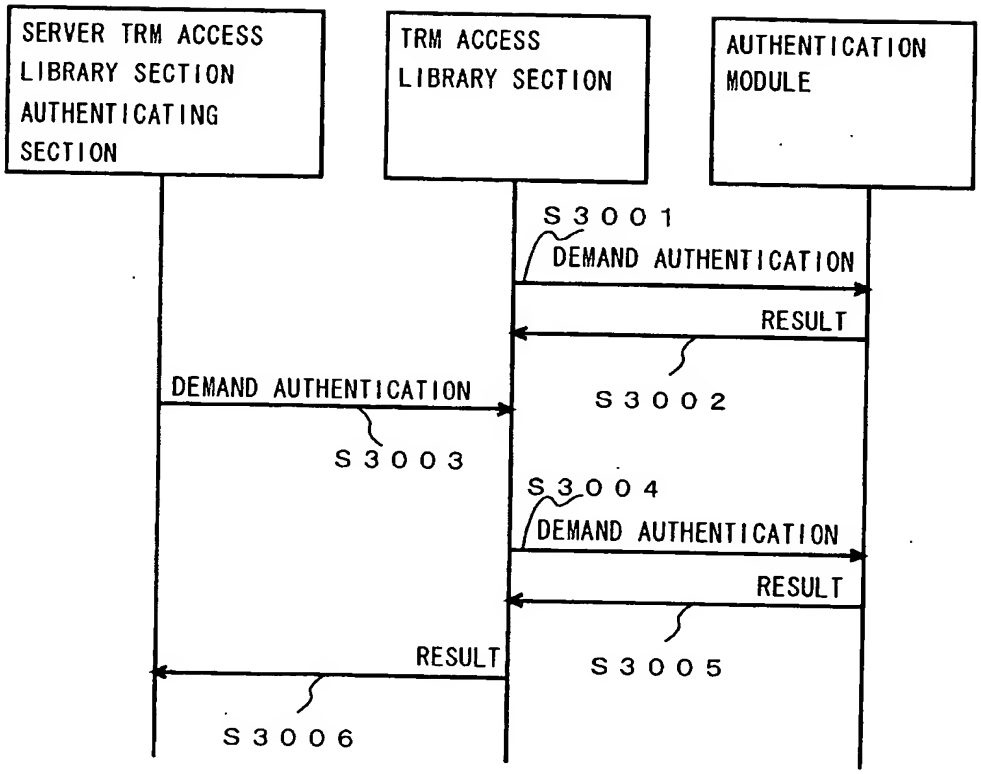

SERVER TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION
AUTHENTICATION MODULE
S3001
DEMAND AUTHENTICATION
RESULT
S3002
DEMAND AUTHENTICATION
S3003
S3004
DEMAND AUTHENTICATION
RESULT
S3005
RESULT
S3006

FIG. 31

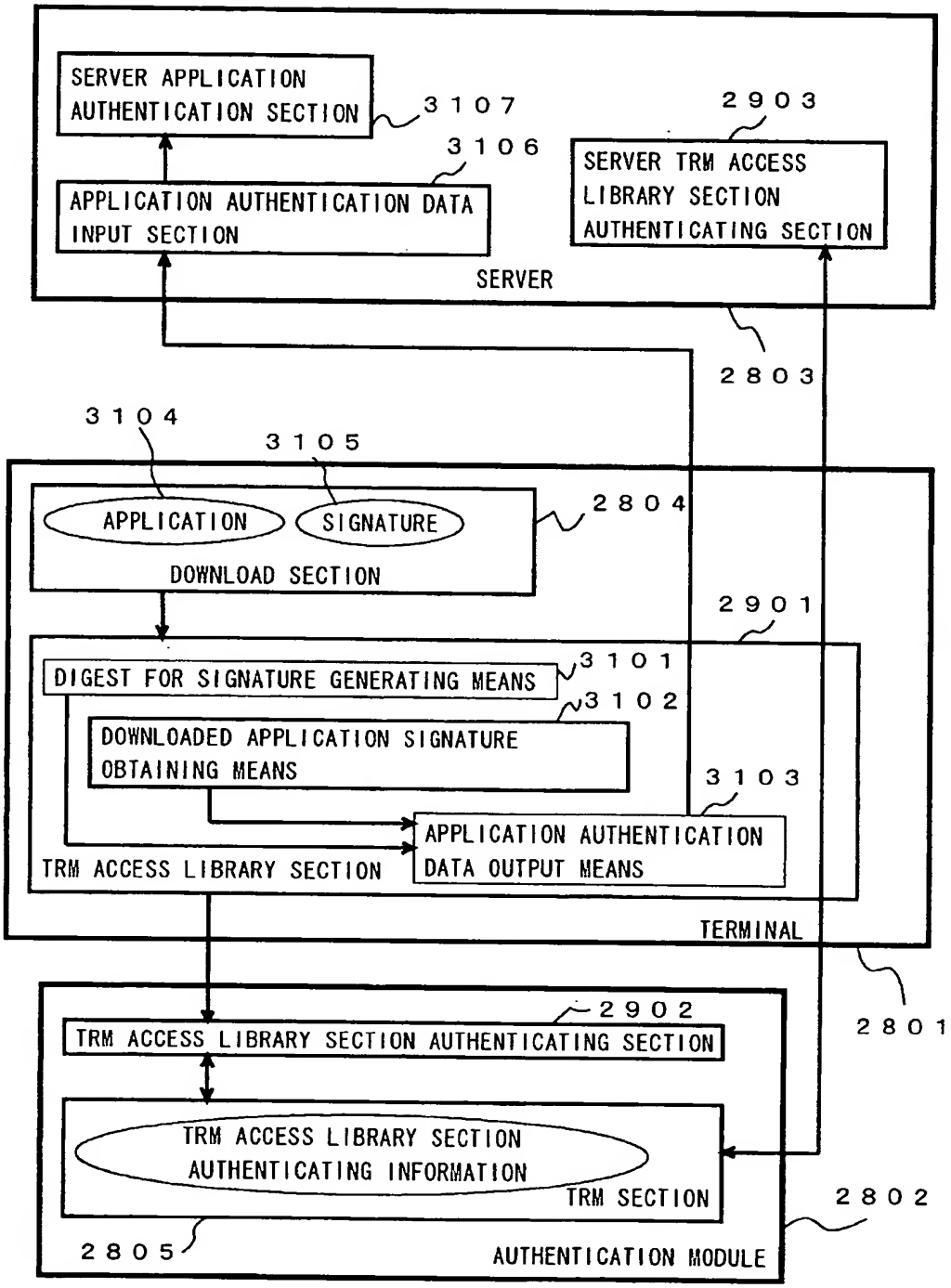

SERVER APPLICATION AUTHENTICATION SECTION
3107
2903
3106
SERVER TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
APPLICATION AUTHENTICATION DATA INPUT SECTION
SERVER
2803
3104
3105
APPLICATION
SIGNATURE
2804
DOWNLOAD SECTION
2901
DIGEST FOR SIGNATURE GENERATING MEANS
3101
3102
DOWNLOADED APPLICATION SIGNATURE OBTAINING MEANS
3103
APPLICATION AUTHENTICATION DATA OUTPUT MEANS
TRM ACCESS LIBRARY SECTION
TERMINAL
2801
2902
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATING INFORMATION
TRM SECTION
2802
2805
AUTHENTICATION MODULE

FIG. 32

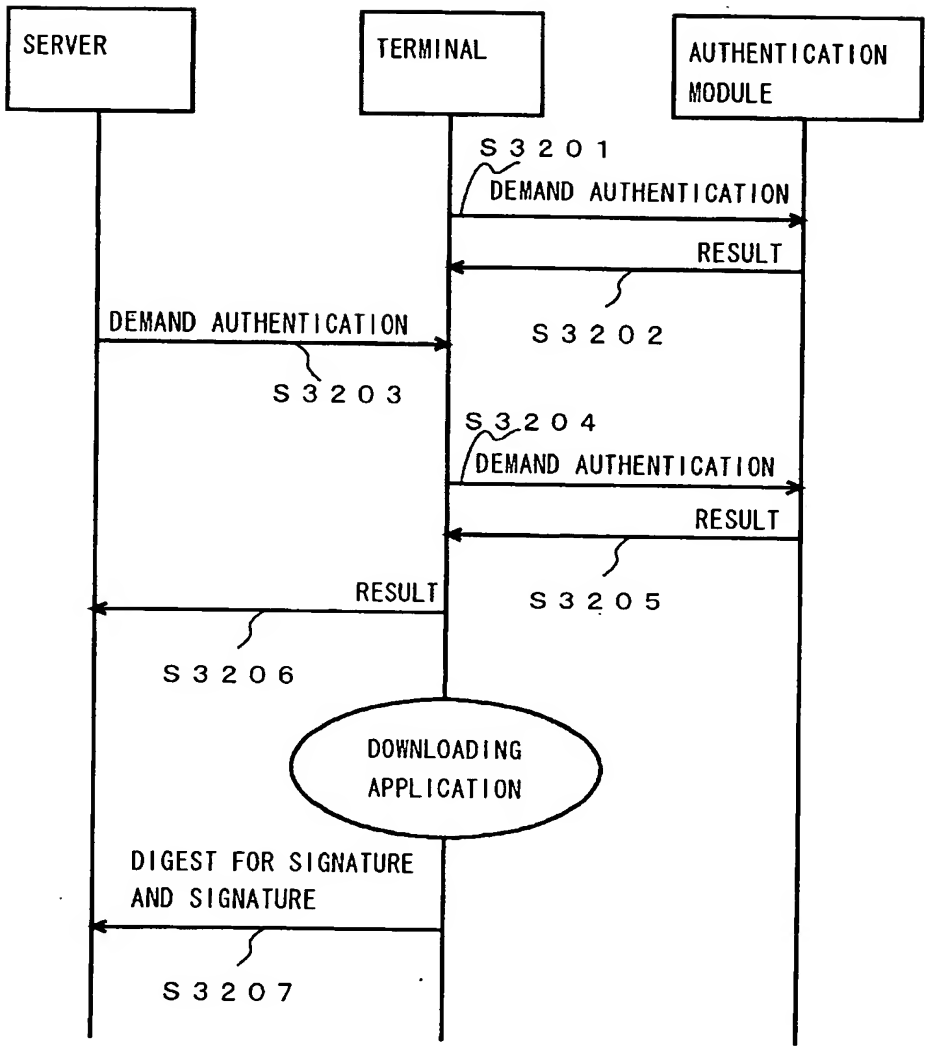

SERVER
TERMINAL
AUTHENTICATION MODULE
S3201
DEMAND AUTHENTICATION
RESULT
S3202
DEMAND AUTHENTICATION
S3203
S3204
DEMAND AUTHENTICATION
RESULT
S3205
RESULT
S3206
DOWNLOADING APPLICATION
DIGEST FOR SIGNATURE AND SIGNATURE
S3207

FIG. 33

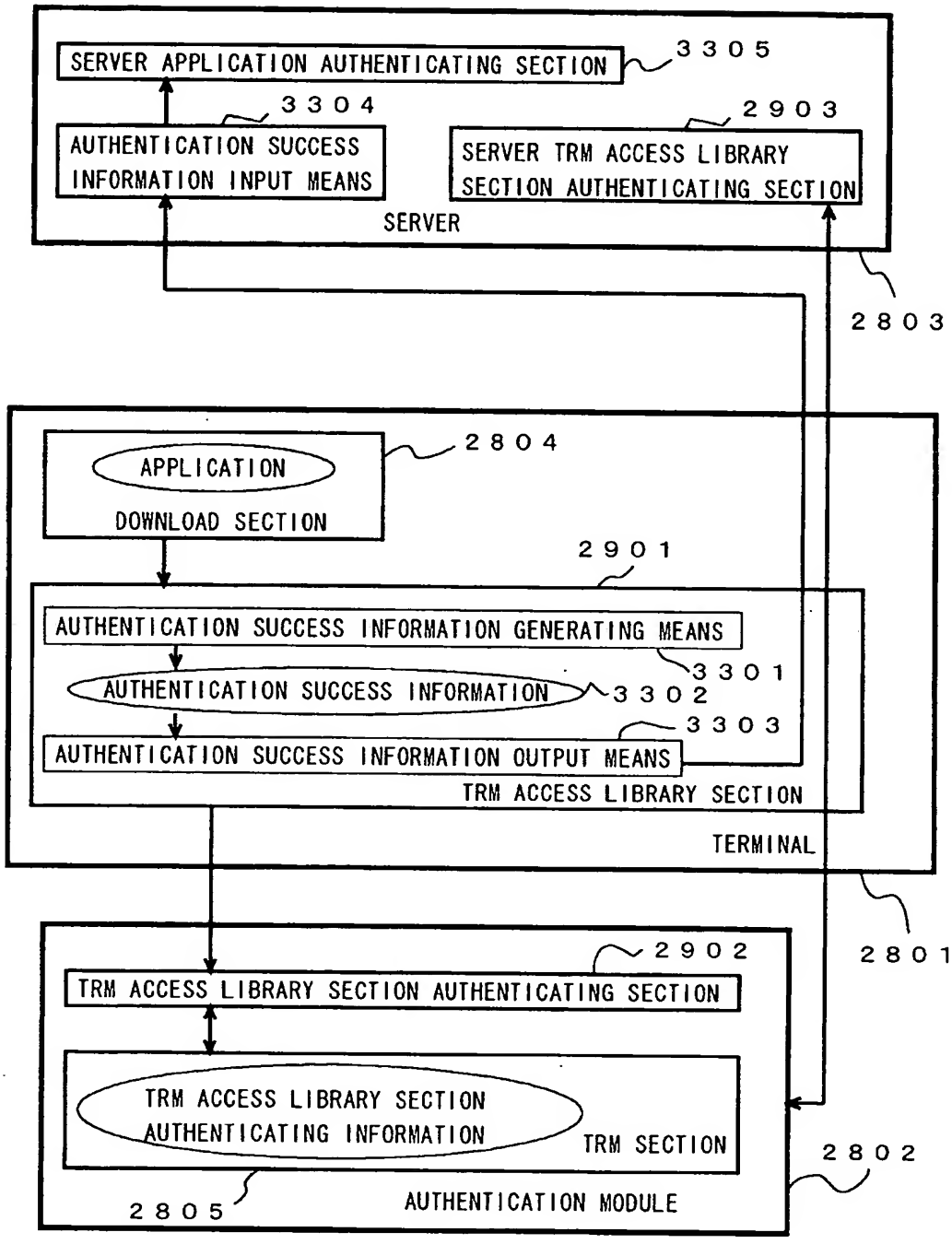

SERVER APPLICATION AUTHENTICATING SECTION
3305
3304
AUTHENTICATION SUCCESS INFORMATION INPUT MEANS
2903
SERVER TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
SERVER
2803
2804
APPLICATION DOWNLOAD SECTION
2901
AUTHENTICATION SUCCESS INFORMATION GENERATING MEANS
3301
AUTHENTICATION SUCCESS INFORMATION
3302
3303
AUTHENTICATION SUCCESS INFORMATION OUTPUT MEANS
TRM ACCESS LIBRARY SECTION
TERMINAL
2801
2902
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
TRM ACCESS LIBRARY SECTION AUTHENTICATING INFORMATION
TRM SECTION
2802
2805
AUTHENTICATION MODULE

FIG. 3 4

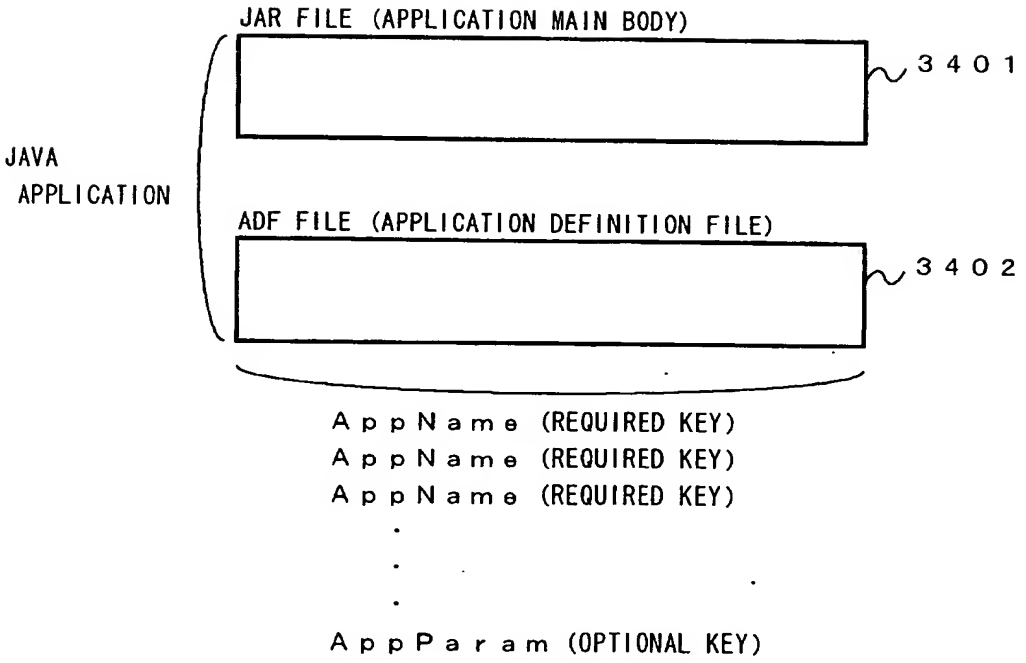

JAR FILE (APPLICATION MAIN BODY)
3401
JAVA APPLICATION
ADF FILE (APPLICATION DEFINITION FILE)
3402
AppName (REQUIRED KEY)
AppName (REQUIRED KEY)
AppName (REQUIRED KEY)
AppParam (OPTIONAL KEY)

FIG. 35

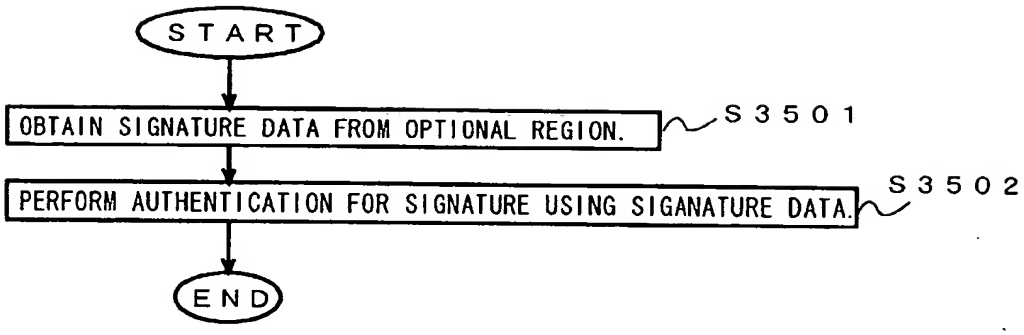

START
OBTAIN SIGNATURE DATA FROM OPTIONAL REGION.
S3501
PERFORM AUTHENTICATION FOR SIGNATURE USING SIGANATURE DATA.
S3502
END

FIG. 36

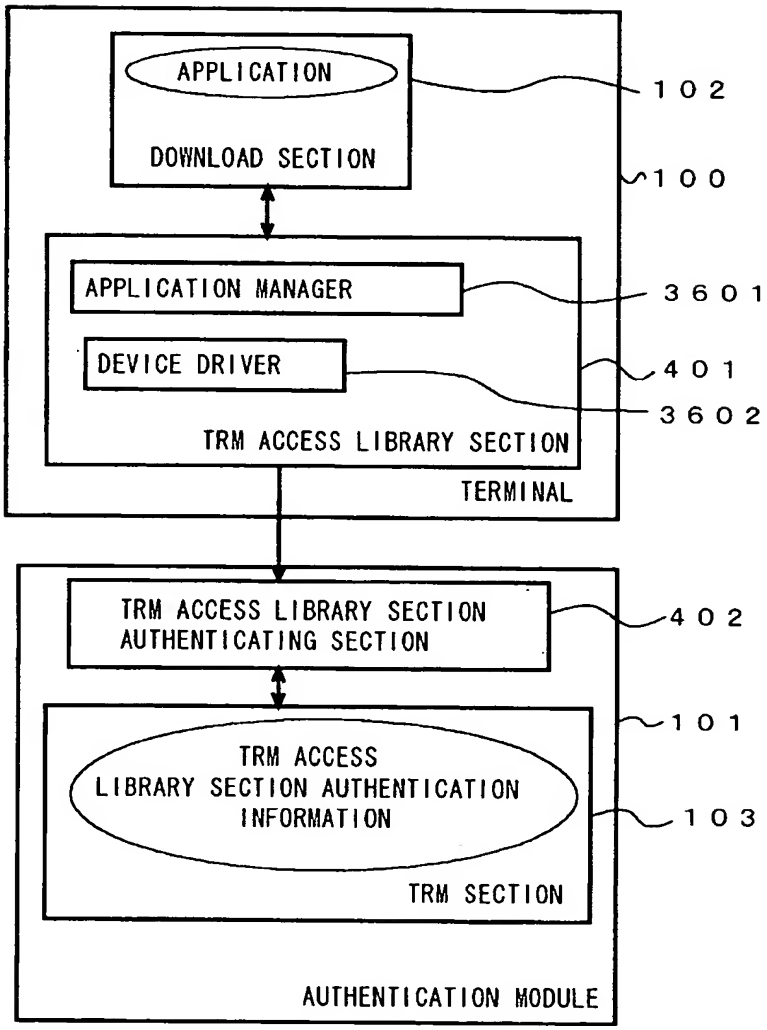

APPLICATION
102
DOWNLOAD SECTION
100
APPLICATION MANAGER
3601
DEVICE DRIVER
401
3602
TRM ACCESS LIBRARY SECTION
TERMINAL
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
402
101
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
103
TRM SECTION
AUTHENTICATION MODULE

FIG. 37

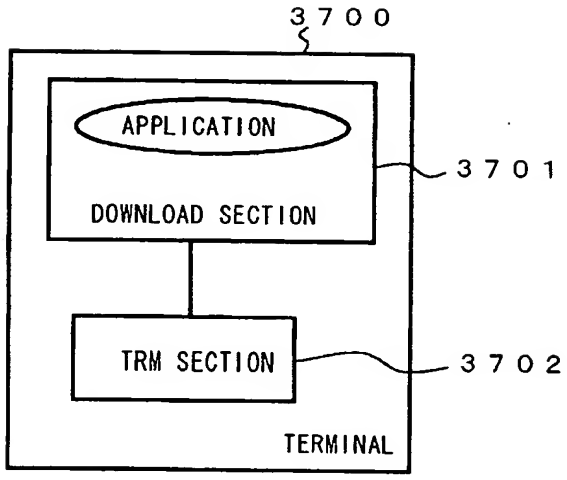

3700
APPLICATION
DOWNLOAD SECTION
3701
TRM SECTION
3702
TERMINAL

FIG. 38

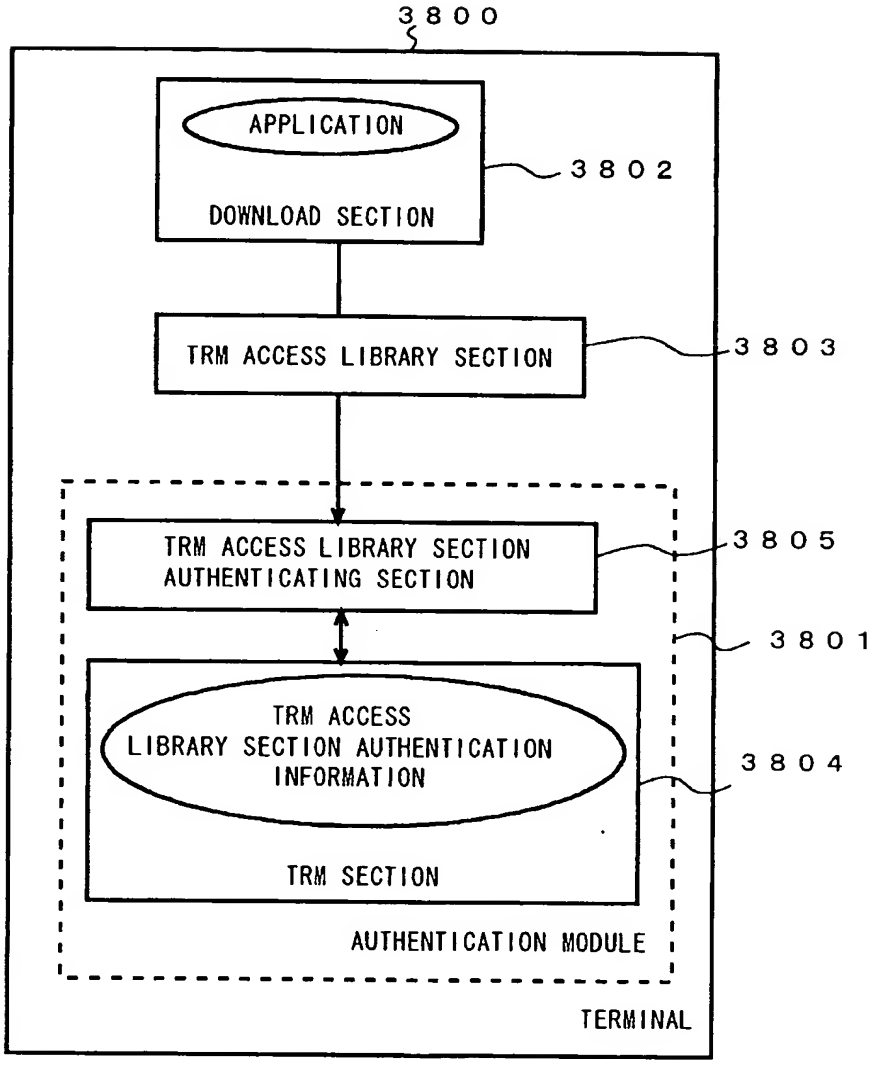

3800
APPLICATION
DOWNLOAD SECTION
3802
TRM ACCESS LIBRARY SECTION
3803
TRM ACCESS LIBRARY SECTION AUTHENTICATING SECTION
3805
3801
TRM ACCESS LIBRARY SECTION AUTHENTICATION INFORMATION
3804
TRM SECTION
AUTHENTICATION MODULE
TERMINAL

FIG. 39

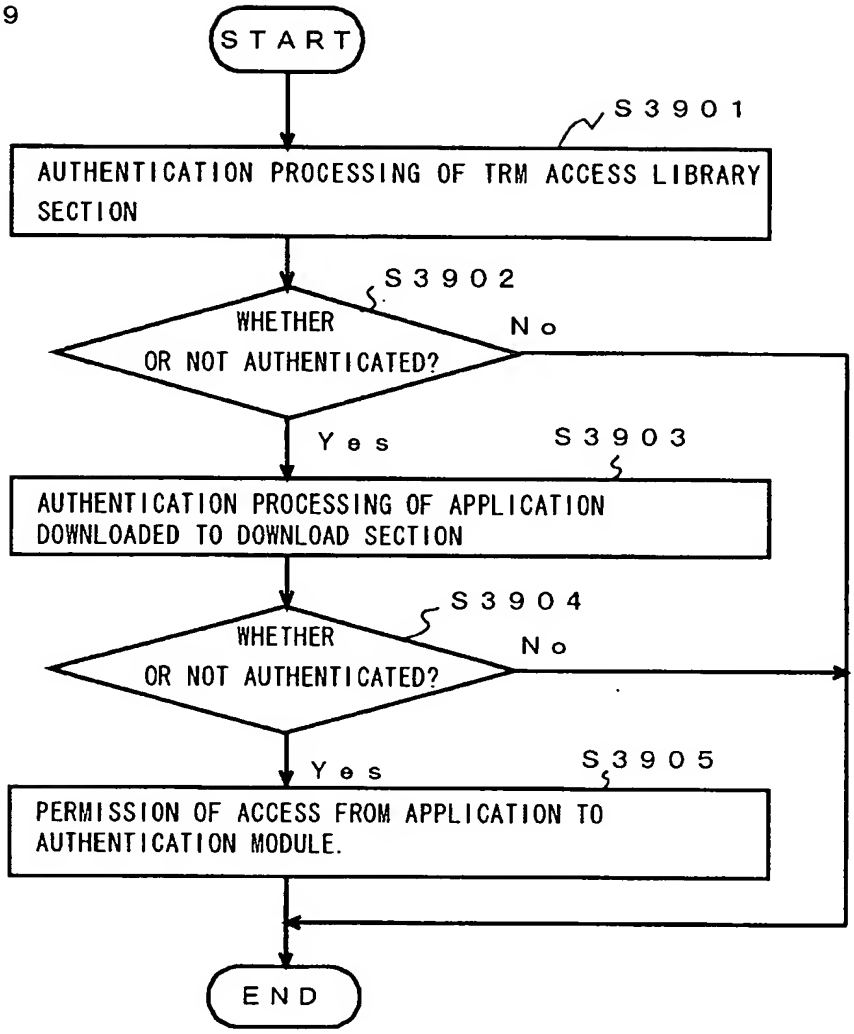

START
S3901
AUTHENTICATION PROCESSING OF TRM ACCESS LIBRARY SECTION
S3902
WHETHER OR NOT AUTHENTICATED?
No
Yes
S3903
AUTHENTICATION PROCESSING OF APPLICATION DOWNLOADED TO DOWNLOAD SECTION
S3904
WHETHER OR NOT AUTHENTICATED?
No
Yes
S3905
PERMISSION OF ACCESS FROM APPLICATION TO AUTHENTICATION MODULE.
END

FIG. 4 0

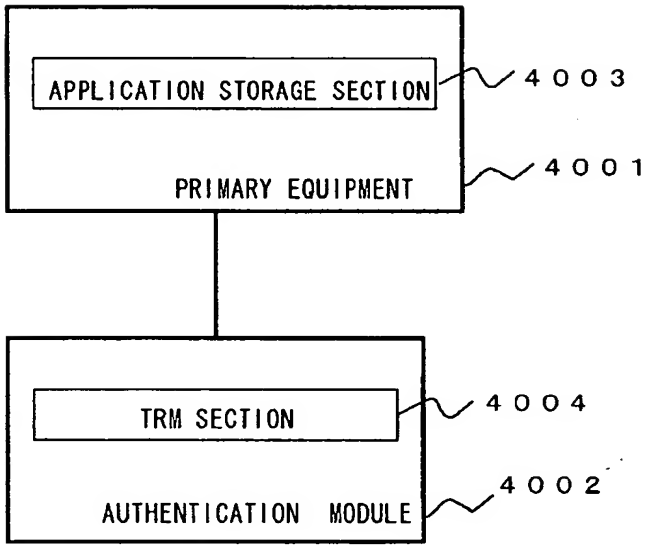

APPLICATION STORAGE SECTION
4003
PRIMARY EQUIPMENT
4001
TRM SECTION
4004
AUTHENTICATION MODULE
4002

FIG. 4 1

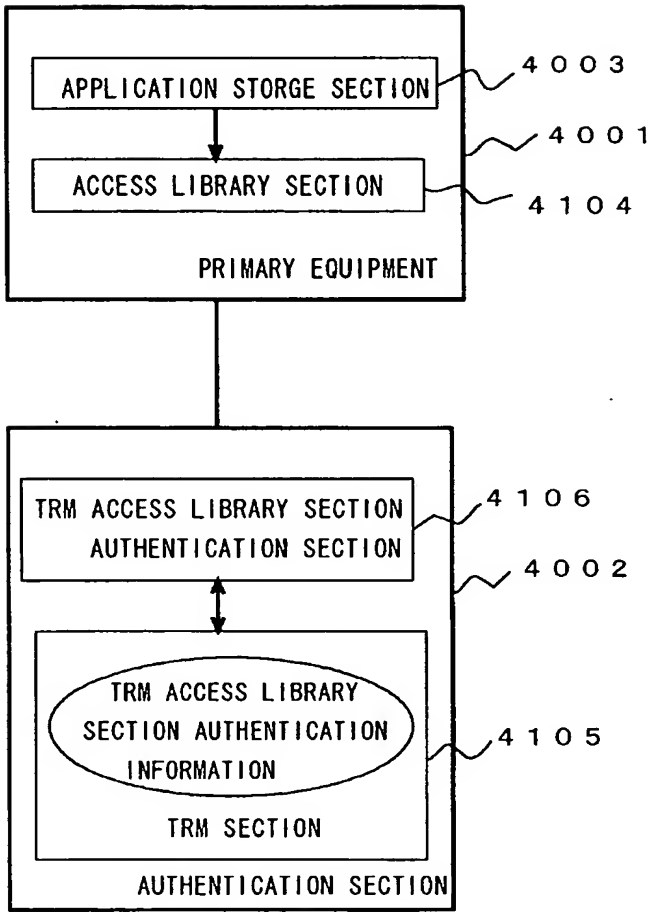

APPLICATION STORGE SECTION
4003
4001
ACCESS LIBRARY SECTION
4104
PRIMARY EQUIPMENT
TRM ACCESS LIBRARY SECTION
AUTHENTICATION SECTION
4106
4002
TRM ACCESS LIBRARY
SECTION AUTHENTICATION
INFORMATION
4105
TRM SECTION
AUTHENTICATION SECTION

FIG. 4 2

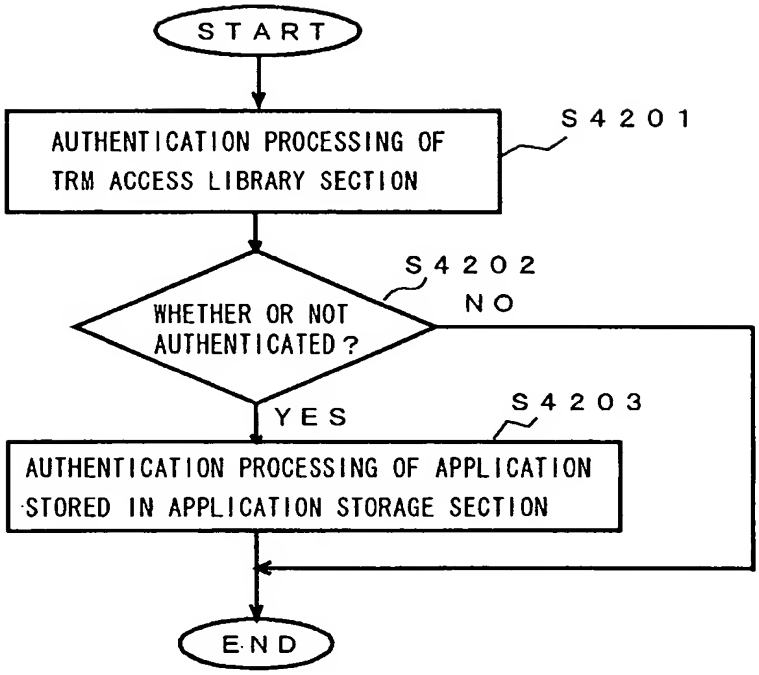

START
AUTHENTICATION PROCESSING OF TRM ACCESS LIBRARY SECTION
S 4 2 0 1
WHETHER OR NOT AUTHENTICATED ?
S 4 2 0 2
NO
YES
S 4 2 0 3
AUTHENTICATION PROCESSING OF APPLICATION STORED IN APPLICATION STORAGE SECTION
END

FIG. 43

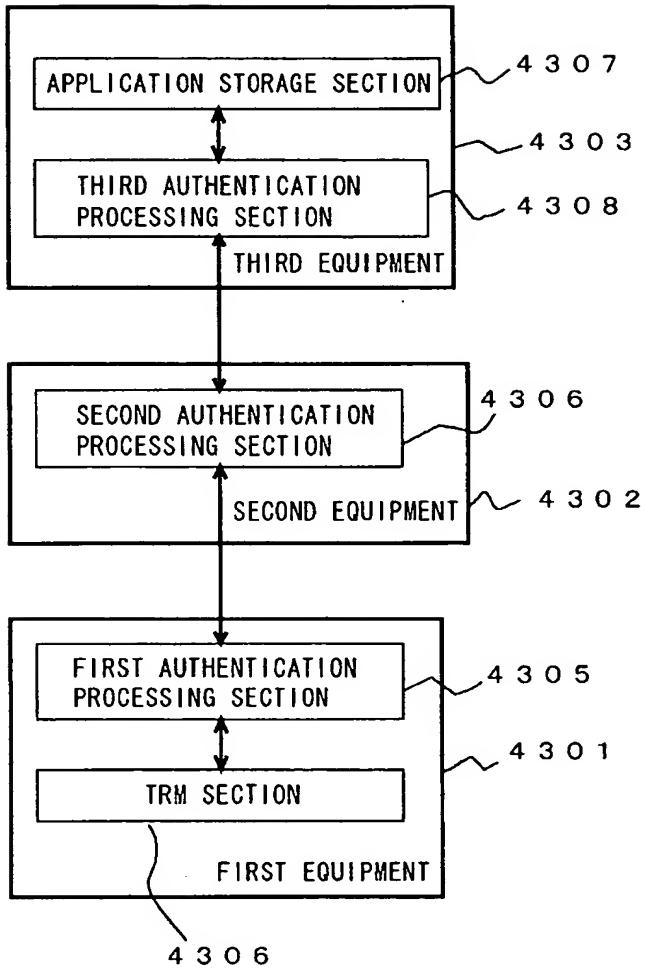

APPLICATION STORAGE SECTION
4307
4303
THIRD AUTHENTICATION PROCESSING SECTION
4308
THIRD EQUIPMENT
SECOND AUTHENTICATION PROCESSING SECTION
4306
SECOND EQUIPMENT
4302
FIRST AUTHENTICATION PROCESSING SECTION
4305
4301
TRM SECTION
FIRST EQUIPMENT
4306

FIG. 44

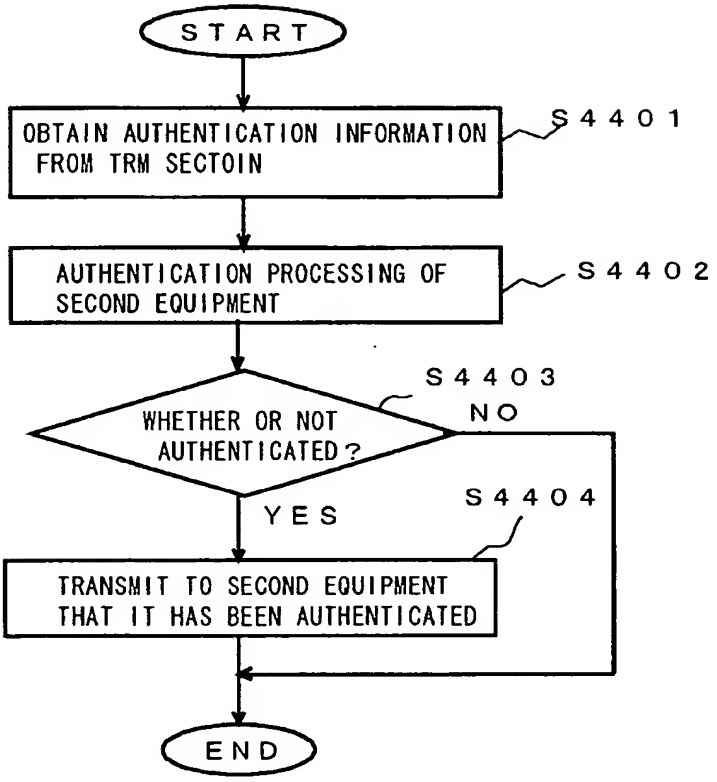

START
OBTAIN AUTHENTICATION INFORMATION FROM TRM SECTOIN
S4401
AUTHENTICATION PROCESSING OF SECOND EQUIPMENT
S4402
WHETHER OR NOT AUTHENTICATED?
S4403
NO
YES
S4404
TRANSMIT TO SECOND EQUIPMENT THAT IT HAS BEEN AUTHENTICATED
END

FIG. 45

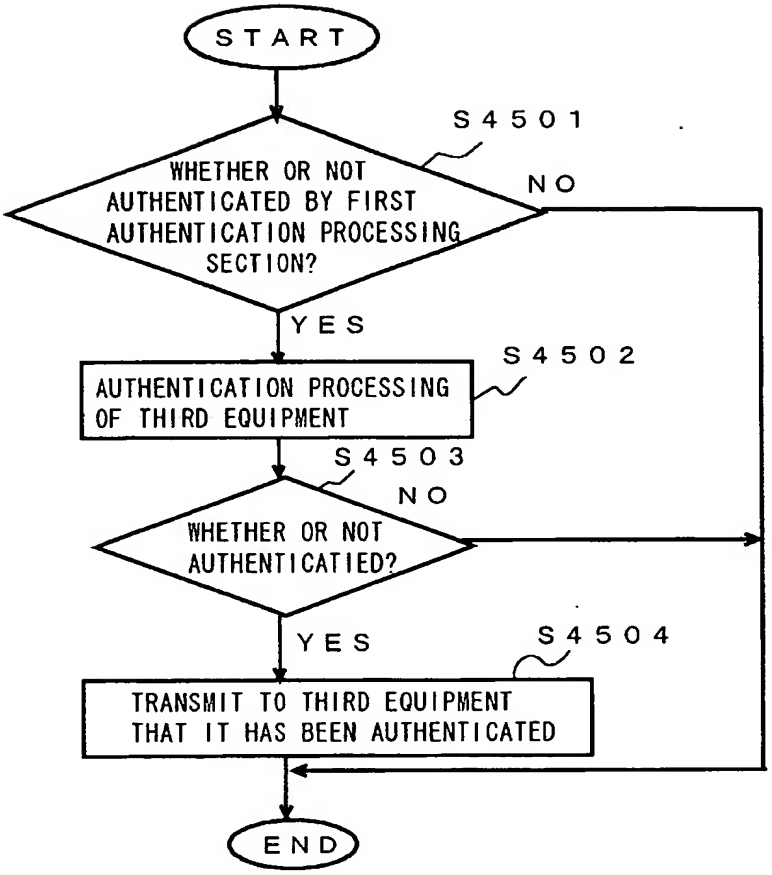

START
S4501
WHETHER OR NOT AUTHENTICATED BY FIRST AUTHENTICATION PROCESSING SECTION?
NO
YES
S4502
AUTHENTICATION PROCESSING OF THIRD EQUIPMENT
S4503
NO
WHETHER OR NOT AUTHENTICATIED?
YES
S4504
TRANSMIT TO THIRD EQUIPMENT THAT IT HAS BEEN AUTHENTICATED
END

FIG. 46

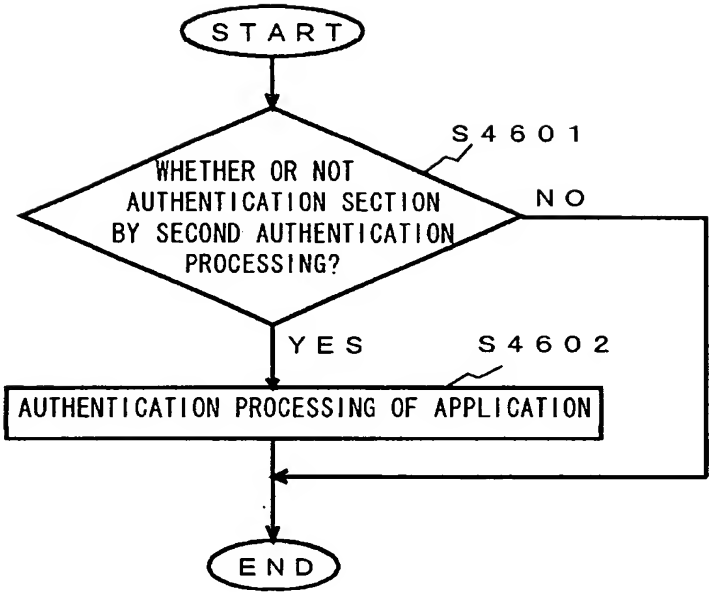

START
S4601
WHETHER OR NOT AUTHENTICATION SECTION BY SECOND AUTHENTICATION PROCESSING?
NO
YES
S4602
AUTHENTICATION PROCESSING OF APPLICATION
END

FIG. 47

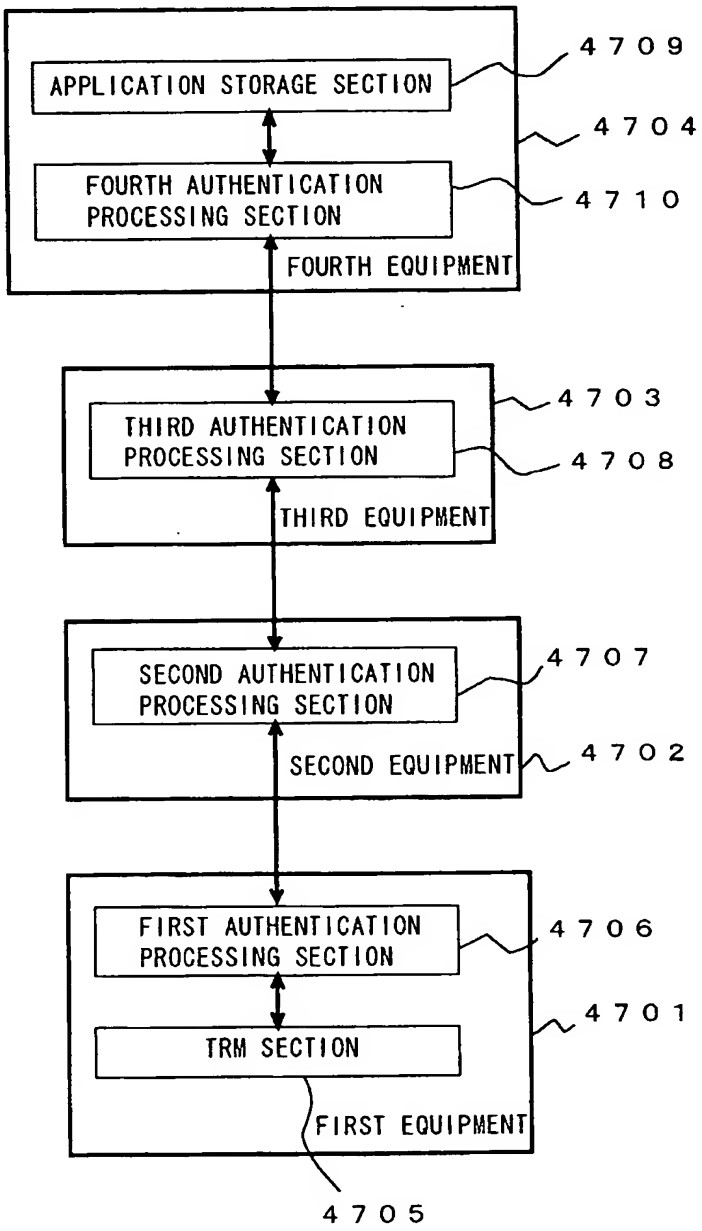

APPLICATION STORAGE SECTION
4709
4704
FOURTH AUTHENTICATION PROCESSING SECTION
4710
FOURTH EQUIPMENT
4703
THIRD AUTHENTICATION PROCESSING SECTION
4708
THIRD EQUIPMENT
SECOND AUTHENTICATION PROCESSING SECTION
4707
SECOND EQUIPMENT
4702
FIRST AUTHENTICATION PROCESSING SECTION
4706
4701
TRM SECTION
FIRST EQUIPMENT
4705

FIG. 48

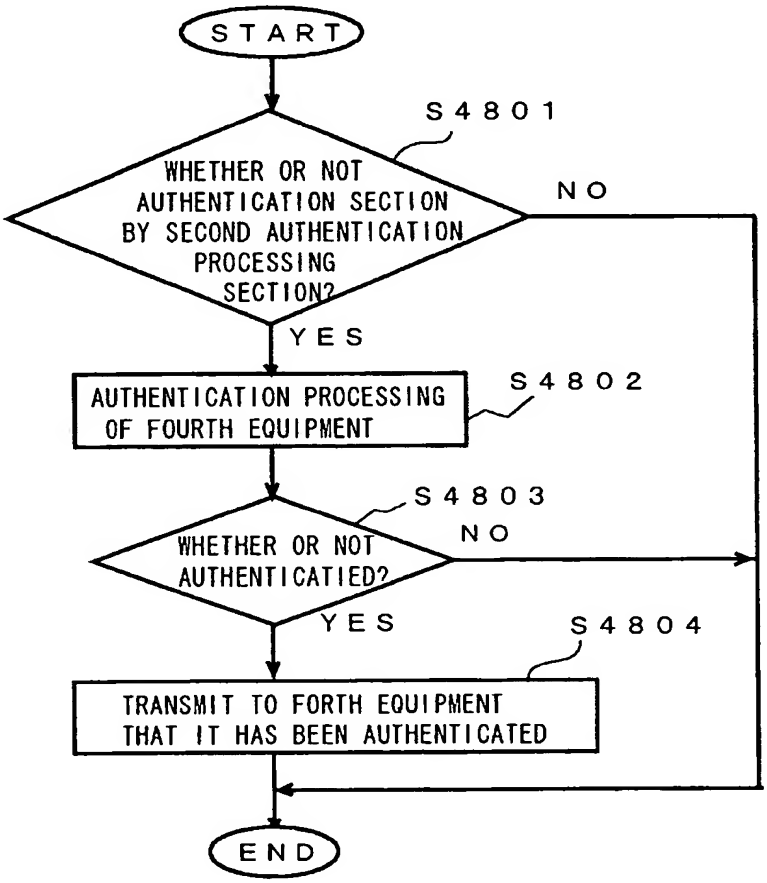

START
S4801
WHETHER OR NOT AUTHENTICATION SECTION BY SECOND AUTHENTICATION PROCESSING SECTION?
NO
YES
AUTHENTICATION PROCESSING OF FOURTH EQUIPMENT
S4802
S4803
WHETHER OR NOT AUTHENTICATIED?
NO
YES
S4804
TRANSMIT TO FORTH EQUIPMENT THAT IT HAS BEEN AUTHENTICATED
END

FIG. 49

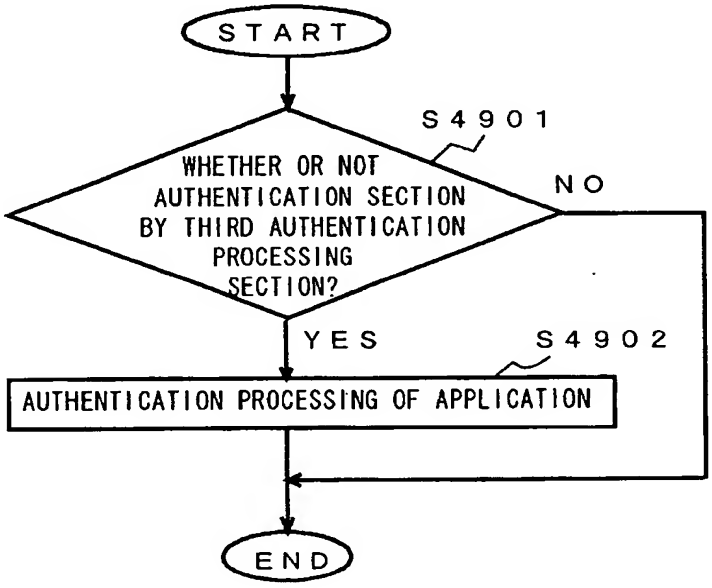

START
S4901
WHETHER OR NOT AUTHENTICATION SECTION BY THIRD AUTHENTICATION PROCESSING SECTION?
NO
YES
S4902
AUTHENTICATION PROCESSING OF APPLICATION
END

FIG. 50

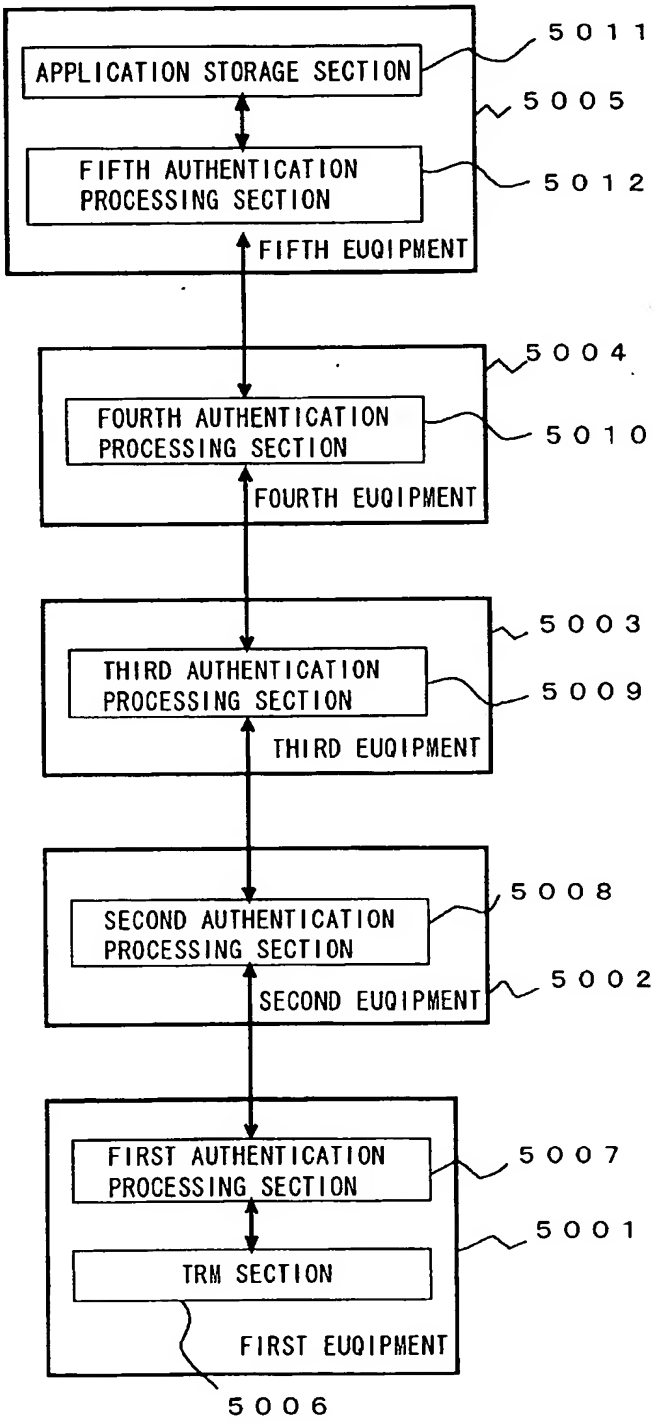

APPLICATION STORAGE SECTION
5011
5005
FIFTH AUTHENTICATION PROCESSING SECTION
5012
FIFTH EUQIPMENT
5004
FOURTH AUTHENTICATION PROCESSING SECTION
5010
FOURTH EUQIPMENT
5003
THIRD AUTHENTICATION PROCESSING SECTION
5009
THIRD EUQIPMENT
5008
SECOND AUTHENTICATION PROCESSING SECTION
5002
SECOND EUQIPMENT
FIRST AUTHENTICATION PROCESSING SECTION
5007
5001
TRM SECTION
FIRST EUQIPMENT
5006

FIG. 5 1

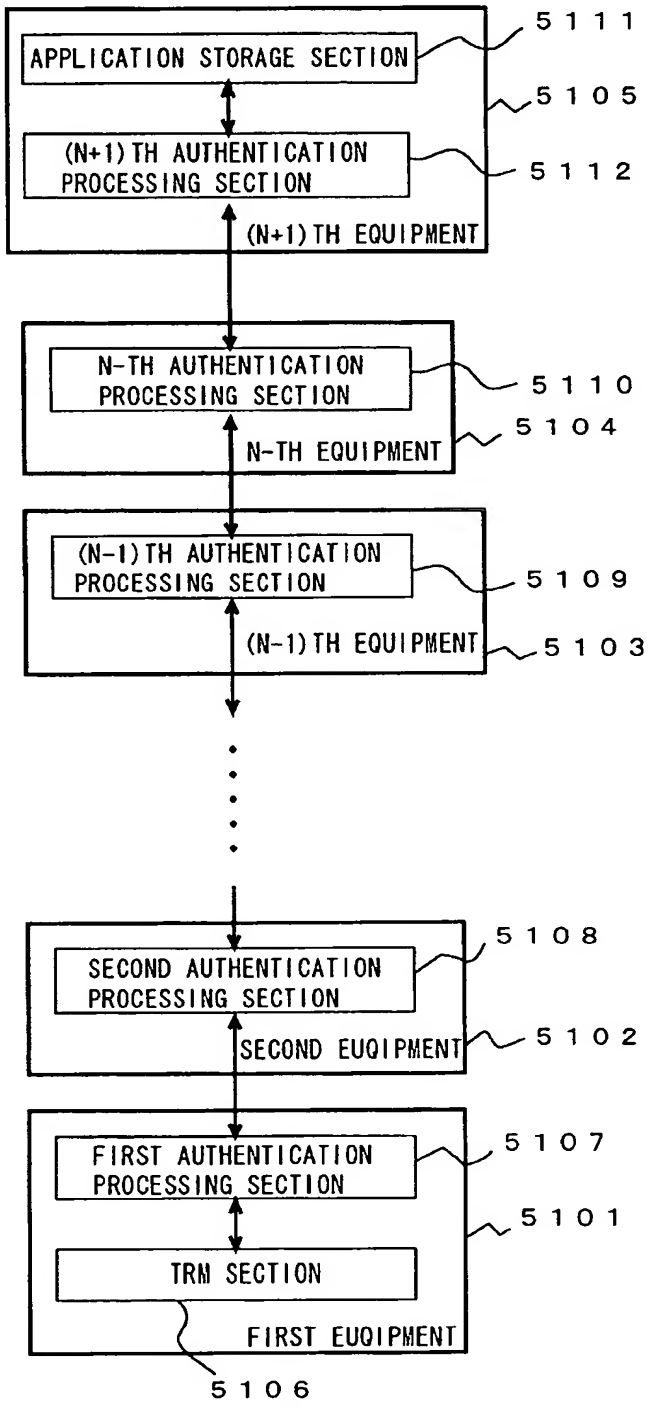

APPLICATION STORAGE SECTION
5111
5105
(N+1)TH AUTHENTICATION PROCESSING SECTION
5112
(N+1)TH EQUIPMENT
N-TH AUTHENTICATION PROCESSING SECTION
5110
5104
N-TH EQUIPMENT
(N-1)TH AUTHENTICATION PROCESSING SECTION
5109
(N-1)TH EQUIPMENT
5103
SECOND AUTHENTICATION PROCESSING SECTION
5108
SECOND EUQIPMENT
5102
FIRST AUTHENTICATION PROCESSING SECTION
5107
5101
TRM SECTION
FIRST EUQIPMENT
5106

FIG. 52

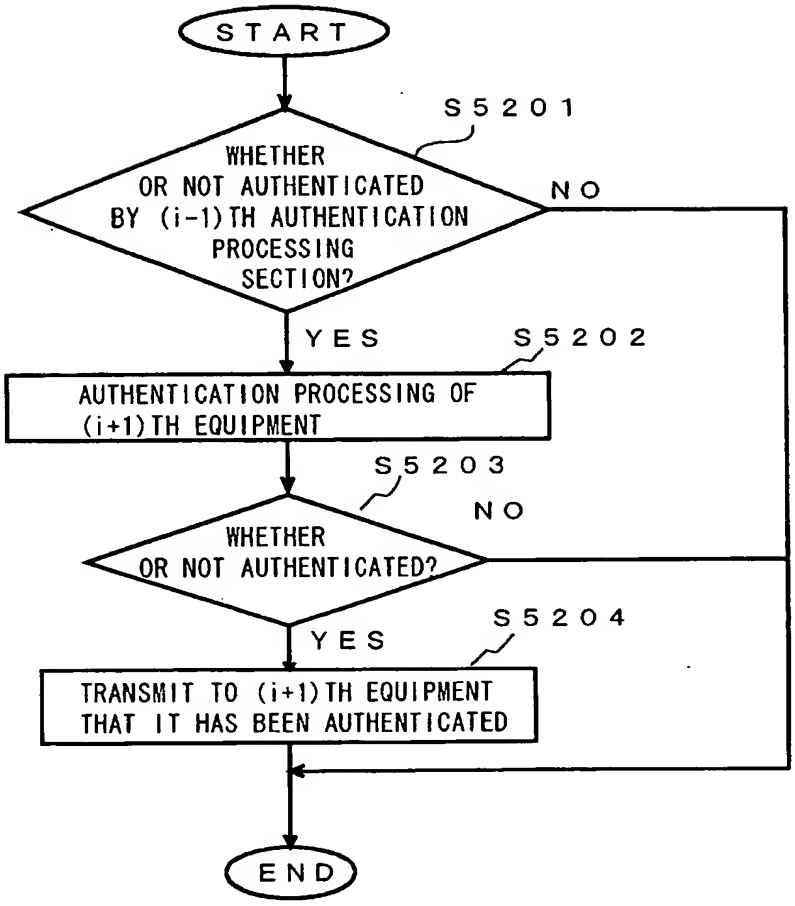

START
S5201
WHETHER OR NOT AUTHENTICATED BY (i-1)TH AUTHENTICATION PROCESSING SECTION?
NO
YES
S5202
AUTHENTICATION PROCESSING OF (i+1)TH EQUIPMENT
S5203
NO
WHETHER OR NOT AUTHENTICATED?
YES
S5204
TRANSMIT TO (i+1)TH EQUIPMENT THAT IT HAS BEEN AUTHENTICATED
END

FIG. 5 3

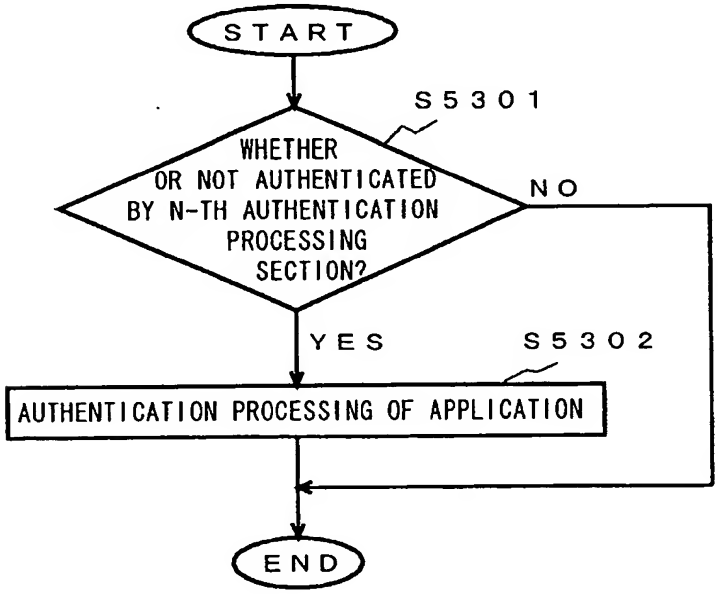

START
S5301
WHETHER OR NOT AUTHENTICATED BY N-TH AUTHENTICATION PROCESSING SECTION?
NO
YES
S5302
AUTHENTICATION PROCESSING OF APPLICATION
END

FIG. 54

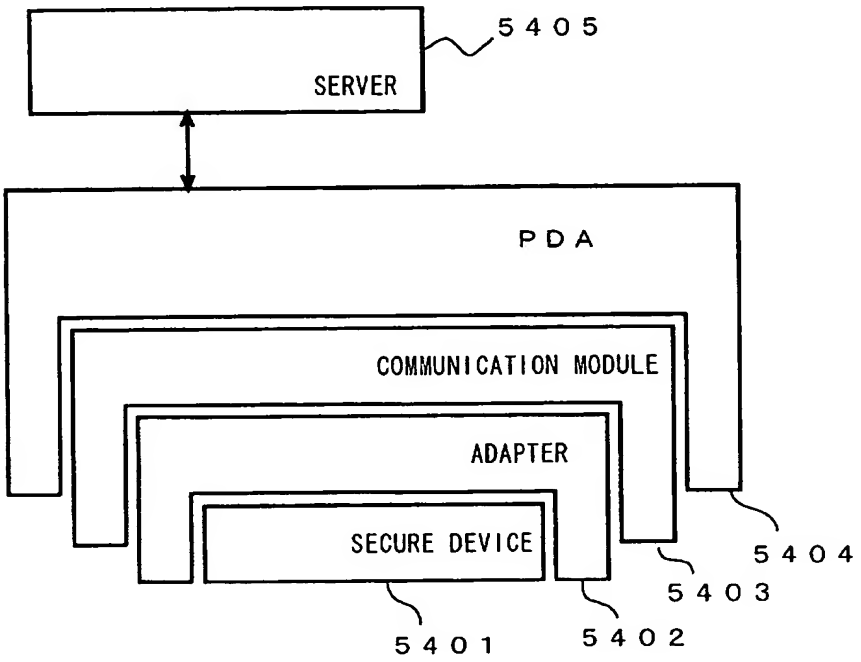
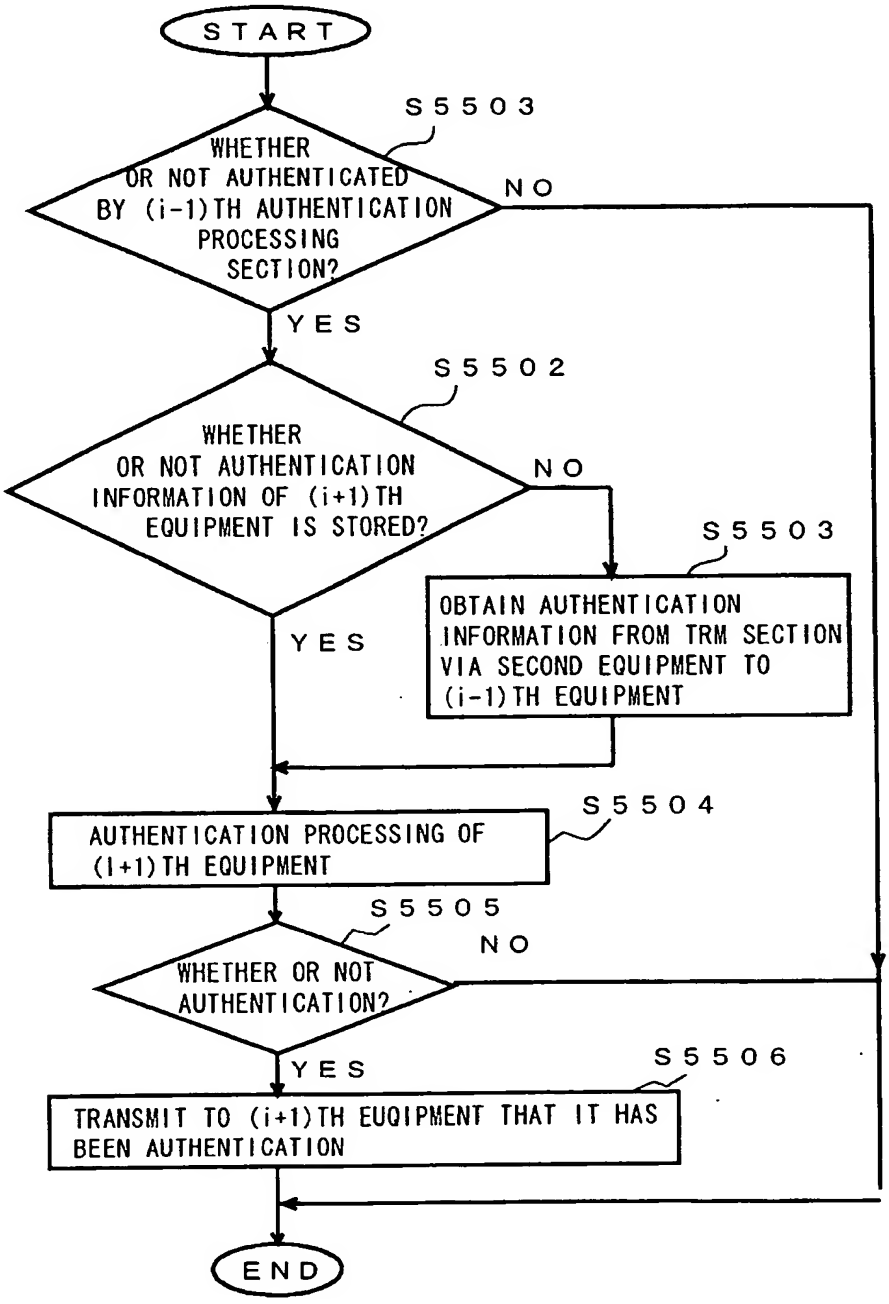

5405
SERVER
PDA
COMMUNICATION MODULE
ADAPTER
SECURE DEVICE
5404
5403
5401
5402

FIG. 55


START
S5503
WHETHER OR NOT AUTHENTICATED BY (i-1)TH AUTHENTICATION PROCESSING SECTION?
NO
YES
S5502
WHETHER OR NOT AUTHENTICATION INFORMATION OF (i+1)TH EQUIPMENT IS STORED?
NO
S5503
OBTAIN AUTHENTICATION INFORMATION FROM TRM SECTION VIA SECOND EQUIPMENT TO (i-1)TH EQUIPMENT
YES
S5504
AUTHENTICATION PROCESSING OF (i+1)TH EQUIPMENT
S5505
WHETHER OR NOT AUTHENTICATION?
NO
YES
S5506
TRANSMIT TO (i+1)TH EUQIPMENT THAT IT HAS BEEN AUTHENTICATION
END